



Universidade de Brasília
Faculdade de Direito

Eduarda Costa Almeida

**DIGA-ME OS SEUS DADOS, QUE EU LHE DIREI QUEM VOCÊ VAI SER: O
DIREITO À EXPLICAÇÃO COMO GARANTIA DA AUTODETERMINAÇÃO
INFORMATIVA NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

Brasília – DF

2023

EDUARDA COSTA ALMEIDA

Diga-me os seus dados, que eu lhe direi quem você vai ser: o direito à explicação como garantia da autodeterminação informativa na lei geral de proteção de dados pessoais.

Monografia apresentada à Faculdade de
Direito como requisito parcial à obtenção
do título de Bacharel em Direito.

Professor Orientador: Doutor Alexandre
Kehrig Veronese Aguiar

Brasília – DF
2023

EDUARDA COSTA ALMEIDA

Diga-me os seus dados, que eu lhe direi quem você vai ser: o direito à explicação como garantia da autodeterminação informativa na lei geral de proteção de dados pessoais.

A Comissão Examinadora, abaixo identificada, [reprova/aprova] o Trabalho de Conclusão do Curso de Direito da Universidade de Brasília da aluna

Eduarda Costa Almeida

Doutor Alexandre Veronese
Professor-Orientador

Doutora Miriam Wimmer
Membro da Comissão Examinadora

Doutora Veridiana Alimonti
Membro da Comissão Examinadora

Brasília

RESUMO

A todo momento, titulares de dados ou cidadãos interessados estão sendo impactados por decisões automatizadas tomadas com base em dados pessoais para acesso a produtos e serviços oferecidos por entidades públicas ou privadas. A Lei Geral de Proteção de Dados determina um direito de receber informações sobre os critérios e procedimentos utilizados na decisão automatizada sempre que ela afetar os interesses das pessoas, um direito à explicação. Esse direito é uma das facetas da autodeterminação informativa, enquanto fundamento de proteção de dados. Ao mesmo tempo que esse conceito tem sido ressignificado, ele influencia sobremaneira a interpretação da lei, principalmente seus princípios e direitos. O direito à explicação surge como ferramenta para se compreender o processo de tomada de decisão automatizada e, com isso, poder garantir os outros direitos ao titular. A hipótese dessa pesquisa é de que existem fronteiras a esse direito e que a percepção da sua existência, de acordo com a lei brasileira, não é suficiente para garantia plena da autodeterminação. Para compreender a extensão de um direito à explicação no Brasil, analisou-se as leis de proteção de dados da União Europeia, Uruguai e Colômbia, em vista dos consensos e divergências em regular esse tema. As barreiras na garantia à autodeterminação informativa se impõem enquanto desafios para concretização do direito, como dar transparência a um sistema complexo e desenvolvido em um contexto de *big data*, além dos interesses éticos e comerciais na explicação.

Palavras-chave: decisão automatizada; dados pessoais; autodeterminação informativa; direito à explicação.

LISTA DE QUADROS

- Figura 1 - Fluxograma do funcionamento de sistemas de IA
- Figura 2 - Tabela das formas de aprendizado em *machine learning*
- Figura 3 - Quadro sobre a relação entre IA, *machine learning* e *deep learning*
- Figura 4 - Conceito de decisão automatizada na LGPD
- Figura 5 - Linha do tempo sobre a autodeterminação e decisão automatizada no projeto de lei da LGPD
- Figura 6 - Diagrama de conceitos relacionados à autodeterminação informativa
- Figura 7 - Tabela associativa dos princípios de proteção de dados da OCDE e da LGPD
- Figura 8 - Tabela sobre a conexão dos direitos previstos no art. 18 da LGPD com a autodeterminação informativa
- Figura 9 - Tabela comparativa das consequências de um direito de informação
- Figura 10 - Checklist do direito à explicação
- Figura 11 - Artigos relevantes para um direito à explicação na UE
- Figura 12 - Artigos relevantes para um direito à explicação no Uruguai
- Figura 13 - Artigos relevantes para um direito à explicação na Colômbia
- Figura 14 - Artigos relevantes para um direito à explicação no Brasil

LISTA DE ABREVIATURA E SIGLAS

- AEPD - Autoridade Europeia para a Proteção de dados (*European Data Protection Supervisor*)
- CEPD - Comitê Europeu de Proteção de Dados (*European Data Protection Board*)
- CDC - Código de Defesa do Consumidor
- Dataprev - Empresa de Tecnologia e Informações da Previdência Social
- EUA - Estados Unidos da América
- FIPP - *Fair Information Practice Principles*
- IA - Inteligência Artificial
- IBGE - Instituto Brasileiro de Geografia e Estatística
- ICO - *Information Commissioner's Office*
- INSS - Instituto Nacional do Seguro Social
- LAI - Lei de Acesso à Informação
- LCP - Lei do Cadastro Positivo
- LGPD - Lei Geral de Proteção de Dados Pessoais
- MCI - Marco Civil da Internet

MJ - Ministério da Justiça

MP - Medida Provisória

OCDE - Organização para Cooperação e Desenvolvimento Econômico

PEC - Proposta de Emenda à Constituição

PL - Projeto de Lei

RGPD - Regulamento Geral sobre a Proteção de Dados

STJ - Superior Tribunal de Justiça

STF - Supremo Tribunal Federal

UE - União Europeia

XAI - *Explainable AI*

SUMÁRIO

1. CONSIDERAÇÕES INICIAIS	8
2. AS DECISÕES AUTOMATIZADAS BASEADAS EM DADOS PESSOAIS	14
2.1. O impacto da Inteligência Artificial na tomada de decisão	16
2.2. Decisões automatizadas reguladas pela LGPD	23
2.3. Casos concretos de decisões automatizadas reguladas pela LGPD	28
2.4. Os influxos da LGPD nas decisões automatizadas	38
3. O SENTIDO ATRIBUÍDO À AUTODETERMINAÇÃO INFORMATIVA NA PROTEÇÃO DE DADOS	42
3.1. A origem do conceito da autodeterminação informativa	42
3.2. A autodeterminação informativa no Brasil	51
3.2.1. A autodeterminação informativa enquanto fundamento da proteção de dados nas normas brasileiras	53
3.2.2. A autodeterminação informativa enquanto conceito base para decisão do Supremo Tribunal Federal	60
3.3. Síntese preliminar da aplicação da autodeterminação informativa na regulação de proteção de dados	64
4. AS IMPLICAÇÕES DA AUTODETERMINAÇÃO INFORMATIVA COMO FUNDAMENTO DA LGPD	71
4.1. Princípios da LGPD relacionados à concretização da autodeterminação informativa	73
4.1.1. Princípios da transparência e do livre acesso	76
4.1.2. Princípios da finalidade, necessidade e adequação	78
4.1.3. Princípios da não discriminação, prevenção, responsabilização e prestação de contas	81
4.2. Direito dos titulares	85
4.2.1. Direito de informação e de acesso aos dados	88
4.2.2. Direito de revisão	93
4.3. Síntese preliminar dos princípios e direitos da LGPD na garantia de uma autodeterminação informativa	97
5. DIREITO À EXPLICAÇÃO	99
5.1. Explicabilidade na proteção de dados	99
5.2. Um direito à explicação em decisões automatizadas baseadas em dados pessoais na União Europeia, Uruguai e Colômbia	111
5.2.1. UE: Regulamento (UE) 2016/276, de 2016	112
5.2.2. Uruguai: Lei nº 18.331, de 2008	118
5.2.3. Colômbia: Lei nº 1.581, de 2012	123
5.3. Um direito à explicação em decisões automatizadas baseadas em dados pessoais na LGPD	127
6. OS LIMITES DO DIREITO À EXPLICAÇÃO NA GARANTIA À AUTODETERMINAÇÃO INFORMATIVA	132
6.1. Barreiras da transparência	133
6.2. Ferramentas explicáveis	138
6.3. Tratamento de dados pessoais na era do Big Data	143

7. CONCLUSÃO	
REFERÊNCIAS	

146
156

1. CONSIDERAÇÕES INICIAIS

As decisões que mais importam para a delimitação dos comportamentos e da personalidade das pessoas, cada vez mais, estão sendo tomadas por algoritmos. Essas ferramentas realizam recomendações de compras, sugestões de opiniões e de atividades culturais, inferências de vontades, formação de perfis, e determinam o acesso a serviços públicos, benefícios sociais ou mesmo o exercício de direitos e liberdades. Em um contexto de *big data*, não cabe mais a apenas um ser humano ou a uma burocracia checar as condições para que uma pessoa execute atividades corriqueiras. Algoritmos decidem a partir do processamento de informações, inclusive pessoais, sobre as condições de um empréstimo bancário, um benefício social ou até os conteúdos direcionados a usuários de redes sociais, por exemplo.

Não há um conceito pacífico sobre o que é *big data*, mas tradicionalmente ele é entendido como ativo de informação com alto volume, alta velocidade e/ou alta variedade, ou seja, é fenômeno o qual permite o processamento massivo de dados de várias fontes em pouco tempo¹. Além disso, não há um mapeamento taxativo das implicações do *big data*, em vista das constantes transformações que esse cenário causa na sociedade e nas relações entre pessoas. A opinião 03/2013 sobre limitação de finalidade do Grupo de Trabalho do Artigo 29 entende o *big data* como fenômeno que se refere ao crescimento exponencial da disponibilidade e da utilização automatizada da informação, inclusive pessoal². Ou seja, refere-se a conjuntos gigantescos de dados detidos por empresas, governos e outras organizações, os quais são então extensivamente analisados por meio de algoritmos computadorizados. O *big data* baseia-se na crescente capacidade da tecnologia para apoiar a coleta e o armazenamento de vastas quantidades de dados, mas também para analisar, compreender e tomar decisões melhor informadas.

No contexto da pandemia do Covid-19, os casos de decisões automatizadas tomadas com base em dados pessoais ganharam ainda mais notoriedade em vista do seu impacto na vida dos brasileiros. Dois exemplos são destacados para ilustrar esse impacto. Por meio da Lei nº 13.982/2020, o Governo Federal implementou uma política de transferência de renda para a parcela mais vulnerável da população diante dos efeitos econômicos da pandemia, o chamado

¹ GARTNET. **Gartner Glossary**. [s.d]. Disponível em:

<https://www.gartner.com/en/information-technology/glossary/big-data>. Acesso em: 19 dez. 2022.

² UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 03/2013 on purpose limitation**. 2013, p. 45. Disponível em:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 13 dez. 2022. Apesar deste guia não ter sido ratificado pelo *European Data Protection Board*, ele ainda é uma fonte de pesquisa relevante para identificação dos parâmetros definidos à época para interpretação da regulação de proteção de dados pessoais.

Auxílio Emergencial. Para que fosse possível identificar as pessoas elegíveis e deferir a concessão do benefício, a Empresa de Tecnologia e Informações da Previdência Social (Dataprev) realizou tratamento automatizado de dados, a partir das informações pessoais. A partir desse tratamento, mais de 68 milhões de cidadãos foram beneficiados pela política³. Além dessa decisão automatizada, a forma de contestar a decisão de recusa do benefício também era automatizada, a qual não era uma revisão da decisão inicial, mas apenas um reprocessamento dos mesmos dados enviados anteriormente⁴.

Nesse mesmo contexto, decisões automatizadas estavam sendo tomadas na moderação de conteúdo em redes sociais, ferramentas utilizadas como portais de notícias sobre os desdobramentos da pandemia e as formas de prevenção da doença. Diante do volume de conteúdos postados em desacordo com os termos de uso das redes sociais, inclusive de desinformação, a moderação de conteúdo, também com base no tratamento de dados pessoais, foi realizada por algoritmos. Essa moderação tinha como finalidade avaliar e remover conteúdos potencialmente nocivos de forma massiva e automatizada, mesmo antes deles serem visualizados por algum usuário⁵. Esse contexto foi intensificado diante das recomendações de distanciamento social, as quais indicavam para o esvaziamento dos escritórios físicos dessas redes sociais e a transferência da execução das atividades de moderação para ferramentas automatizadas⁶. A implementação desses algoritmos, seja pelo setor público ou privado, é consequência do desenvolvimento e disseminação de ferramentas de automação e de Inteligência Artificial (IA), que serão analisadas de forma mais detida no tópico seguinte (tópico 2.1).

O desenvolvimento da tecnologia, principalmente associado ao poder computacional e ao acesso facilitado a dispositivos conectados à internet, e os riscos advindos do uso dessas ferramentas indicaram a necessidade de regulamentar o tratamento de dados pessoais. Entre os anos 1970 e 1980, diferentes normas foram elaboradas no intuito de controlar a tecnologia e garantir direitos aos usuários, principalmente aqueles relacionados à dignidade, autonomia,

³ BRASIL. Ministério da Cidadania. **Auxílio Emergencial 2020**. 2020. Disponível em: <https://aplicacoes.cidadania.gov.br/vis/data3/index.php?g=2>. Acesso em: 12 dez. 2022.

⁴ TAVARES, Clarice *et al.* **O Auxílio Emergencial no Brasil: Desafios na implementação de uma política de proteção social datificada**. 2022, p. 21. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/01_Informe-Brasil_Inteligencia-Artificial-e-Inclusao_PT_22042022.pdf. Acesso em: 15 dez. 2022.

⁵ PEREIRA DA SILVA, Sivaldo; CESAR, Daniel Jorge Teixeira. Inteligência Artificial, moderação de conteúdos no YouTube e a proteção de direitos: características, problemas e impactos políticos. **Liinc em Revista**, Rio de Janeiro, v. 18, n. 2, e6080, nov. 2022, p. 5.

⁶ REDAÇÃO FORBES. Com coronavírus, redes sociais alertam para possíveis erros de moderação de conteúdo. **Forbes**. 2020. Disponível em: <https://forbes.com.br/negocios/2020/03/com-coronavirus-redes-sociais-alertam-para-possiveis-erros-de-moderacao-de-conteudo/>. Acesso em: 15 dez. 2022.

e um direito recém conhecido, a autodeterminação informativa, como cunhado pela Corte Constitucional Alemã, em 1983⁷. Com o passar do tempo, o movimento de regulação da proteção de dados foi se espalhando por diversas regiões do mundo com objetivo de tutelar o fluxo de dados pessoais. Isso ocorreu em vista do vínculo entre os dados pessoais e seus titulares no que tange à capacidade do tratamento dessas informações impactarem diretamente a esfera de direitos dessas pessoas⁸.

No Brasil, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais ou LGPD) foi resultado de um debate multisetorial que levou em conta defensores de direitos humanos, formuladores de políticas públicas, autoridades estatais, empresas de tecnologia, além de outras, em acordo com um debate internacional sobre o tema⁹. Já existiam normas esparsas que tratavam do tema de dados pessoais em contextos específicos no Brasil, a exemplo do Código de Defesa do Consumidor (CDC), da Lei do Cadastro Positivo (LCP), da Lei de Acesso à Informação (LAI), e do Marco Civil da Internet (MCI). No entanto, essas legislações disciplinavam o fluxo de dados pessoais apenas de modo pontual, e, por isso, haveria a necessidade de uma lei geral aplicável a maior parte das relações jurídicas. Assim, a LGPD, em 2018, inaugurou a regulação de proteção de dados pessoais no Brasil com um modelo próximo ao desenvolvido na UE.

Diante da centralidade do tema, em 2022, o Congresso Nacional promulgou a Proposta de Emenda à Constituição (PEC) nº 17/2019, que inseriu a proteção de dados de forma explícita no rol de direitos fundamentais da Constituição Federal de 1988. A PEC, transformada na Emenda à Constituição nº 115/2022, também fixa a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Interessa notar que o Brasil reconheceu a proteção de dados como direito fundamental após a promulgação da LGPD, esse movimento foi diverso daquele feito pela UE. O art. 8º da Carta dos Direitos Fundamentais da UE já reconhecia a proteção de dados pessoais como um direito fundamental desde sua promulgação em 2000. Para sua concretização, a Carta determinou que esse direito seria matéria de uma norma própria para que se pudesse garantir tratamento leal dos dados pessoais

⁷MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado) - Faculdade de Direito da Universidade de Brasília, 2008. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso: 10 nov. 2022, p. 32.

⁸ ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 181.

⁹ DLA PIPER. **Data Protection Laws of the World**. 2022. Disponível em: <https://www.dlapiperdataprotection.com/>. Acesso: 15 jul. 2022.

e para fins específicos. Para tanto, a Diretiva 95/46/CE, que foi revogada pelo Regulamento Geral sobre a Proteção de Dados (RGPD), já regulava a matéria.

A estrutura da LGPD foi inspirada no RGPD, por isso a experiência europeia no tema é relevante para o contexto brasileiro. As duas regulações seguem uma racionalidade *ex ante* de proteção, isso significa que todos os dados pessoais são relevantes e são tutelados pela lei. Os dois modelos adotam um conceito amplo de dados pessoais e determinam a necessidade de fundamentar o tratamento em uma hipótese prevista em lei¹⁰. Ainda, em uma análise dos modelos, nota-se que os princípios da matéria, os direitos dos titulares, e a previsão de uma autoridade central de proteção de dados são semelhantes. Essa última disposição é cumprida pela Autoridade Nacional de Proteção de Dados (ANPD) no Brasil, já o sistema da UE é composto pelas autoridades nacionais, pelo Comitê Europeu de Proteção de Dados (CEPD, *European Data Protection Board*), autoridade consultiva para uniformizar a aplicação do RGPD, e pela Autoridade Europeia para a Proteção de dados (AEPD, *European Data Protection Supervisor*), com capacidade fiscalizatória sobre as instituições da UE¹¹.

Por outro lado, as duas normas divergem em outros aspectos. O RGPD especifica os casos em que a elaboração de um relatório de impacto à proteção de dados é obrigatória, ele também reconhece explicitamente um direito ao esquecimento, e, como regra geral, proíbe o uso de dados pessoais para tomada de decisões automatizadas. Esse não é o caminho elencado pela LGPD, como será estudado no tópico seguinte (tópico 2.2). Para além das questões regulatórias de proteção de dados, dispostas de maneira variada nas diversas jurisdições, o desenvolvimento tecnológico impõe novos desafios a serem respondidos pelo sistema normativo de proteção dos cidadãos, como é o caso das decisões automatizadas.

O uso massivo de decisões automatizadas pode indicar para escolhas mais ágeis e personalizadas para o titular de dados, como nos exemplos da concessão do Auxílio Emergencial e da moderação de conteúdo. Se essas decisões dependessem apenas da atividade humana, é provável que o processo demorasse tempo expressivo e não fosse aplicado de forma padronizada a todos os afetados. Porém, essas decisões envolvem riscos já identificados em casos concretos e a LGPD, entre outros objetivos, também busca mitigá-los. Para tanto, todo o arcabouço regulatório incide sobre esse tipo de tratamento de dados, como os princípios, direitos dos titulares e capacidade fiscalizatória da ANPD. O §1º, do art. 20, da

¹⁰ 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**. vol. 124. ano 28, p. 157-180. São Paulo: ed. RT, jul.-ago. 2019, p. 171

¹¹ UNIÃO EUROPEIA. Comissão Europeia. **Data protection in the EU**. s.d. Disponível em: [https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#:~:text=The%20European%20Data%20Protection%20Board.Data%20Protection%20Regulation%20\(GDPR\)](https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#:~:text=The%20European%20Data%20Protection%20Board.Data%20Protection%20Regulation%20(GDPR).). Acesso em: 16 dez. 2022.

lei, prevê que os titulares dos dados devem ser informados sobre os critérios e os procedimentos utilizados em uma decisão automatizada sempre que ele solicitar. Para alguns, esse dispositivo seria suficiente para depreender-se um direito à explicação. Não obstante, ao mesmo tempo, esse direito encontre limites técnicos, jurídicos e práticos, que serão analisados nesta pesquisa (tópico 6).

Diante desse contexto, este trabalho possui a seguinte pergunta de pesquisa: quais os limites de um direito à explicação na tomada de decisão automatizada baseada em dados pessoais previsto na LGPD para garantia da autodeterminação informativa? Tendo como premissa a existência de um direito à explicação, que será explicitada nesta pesquisa, a hipótese fixada é de que existem fronteiras a esse direito e que a sua existência não é suficiente para garantia do fundamento da autodeterminação informativa. O objetivo dessa pesquisa é verificar os limites do direito à explicação das decisões automatizadas na concretização do fundamento da autodeterminação, já que esse conceito não é uma “bala de prata” para resolução de desafios impostos pelos efeitos das decisões automatizadas. Para além da finalidade acadêmica, essa pesquisa visa informar os titulares de dados sobre o estado atual de um direito à explicação quando submetidos a decisões automatizadas. Além disso, este trabalho busca evidenciar as limitações deste direito, para que outros atores sociais possam implementar ferramentas para garantia da autodeterminação diante de seus novos sentidos.

Esta pesquisa possui três eixos fundamentais para a aferição da hipótese levantada, quais sejam: decisão automatizada com base em dados pessoais; autodeterminação informativa; e direito à explicação. As ferramentas técnicas para tomada de decisão automatizada serão estudadas, já que os requisitos legais garantidores da interpretabilidade e explicação da decisão se complexificam com o desenvolvimento de métodos de aprendizagem profunda (*deep learning*) e outros modelos opacos (*black box*). Esses elementos são essenciais para a garantia da racionalidade e confiabilidade do resultado, por isso o mecanismo de decisão também deve ser investigado a fim de compreender-se a extensão técnica dessa explicação¹².

Do ponto de vista jurídico, ainda não há entendimento consolidado sobre as fronteiras de um direito à explicação. Na tentativa de delimitar esse direito, as normas de outras jurisdições serão estudadas para que seja possível analisar outros casos em que haja

¹² BIBAL, Adrien, LOGNOUL, Michael, DE STREEL, Alexandre *et al.* Legal requirements on explainability in machine learning. **Artificial Intelligence Law** 29, 149–169. 2021. Disponível em: <https://doi.org/10.1007/s10506-020-09270-4>. Acesso em: 15 dez. 2022, p. 149.

maturidade na interpretação da lei de proteção de dados. A pesquisa se debruçará sobre as normas da União Europeia, em vista das semelhanças entre a LGPD e o RGPD, do Uruguai e da Colômbia, por serem dois países da América Latina com leis diferentes sobre o tratamento de dados pessoais no que tange às decisões automatizadas, de forma a criar escopos diversos de proteção. Assim, a análise das normas de dados dessas três jurisdições permite o mapeamento de três maneiras diferentes de regular o tema, o que garante insumos consistentes para análise do cenário brasileiro no tema.

A autodeterminação foi escolhida como parâmetro deste estudo por ser um dos pilares para desenvolvimento da matéria de proteção de dados pessoais e garantir ao titular autonomia para desenvolver sua personalidade a partir de seus dados. A LGPD reconhece a autodeterminação informativa como fundamento da lei, o que a torna conceito central para o atingimento dos requisitos de conformidade. Com essa pesquisa, será possível mapear a origem do conceito, os avanços e os limites, além da extensão da autodeterminação e, assim, vislumbrar outras medidas necessárias para a garantia desse fundamento, analisando se esse conceito ainda está sendo perseguido pela matéria de proteção de dados.

Como a lei busca regular um tratamento de dados pessoais que observe os direitos fundamentais, bem como a inovação e o desenvolvimento econômico, garantir a concretude de seus fundamentos é relevante para construção do sistema inaugurado pela LGPD em bases sólidas. Nesse sentido, a autodeterminação informativa pode ser reconhecida como fio condutor na interpretação da lei, de forma a tornar o direito à explicação um vetor de garantia da autodeterminação quando titular é exposto à decisão automatizada. Por isso, esta pesquisa se debruça sobre os desafios do direito à explicação nas decisões automatizadas a fim de perceber em que medida esse direito é suficiente para concretização da autodeterminação.

A metodologia dessa pesquisa será qualitativa, baseada em pesquisa bibliográfica de artigos acadêmicos, artigos jornalísticos, decisões judiciais, documentos elaborados por autoridades de proteção de dados, políticas e relatórios de outros atores sociais, como empresas e entidades da sociedade civil organizada. Na revisão da literatura, serão examinadas as obras nacionais e estrangeiras que versam sobre os três eixos da pesquisa. A partir de uma revisão doutrinária, a análise avançará para a legislação e os documentos publicados pelas autoridades de proteção de dados, a fim de se perceber a aplicação do tema para orientações em casos concretos.

Para que se alcance o objetivo da pesquisa, será necessário, inicialmente, (i) compreender o que é considerado decisão automatizada de acordo com os parâmetros da LGPD (tópico 2.1); (ii) exemplificar decisões automatizadas que afetam rotineiramente os

titulares (tópico 2.2); e (iii) identificar os benefícios e riscos à proteção de dados já evidenciados (tópico 2.3). Após esse tópico, serão analisados o conceito (tópico 3.1) e as implicações (tópico 3.2) do fundamento da autodeterminação informativa na matéria de proteção de dados a fim de se mapear seus influxos nos princípios (tópico 4.1) e direitos dos titulares (tópico 4.2). Por fim, a delimitação das decisões automatizadas (tópico 2) e do sentido de autodeterminação informativa (tópico 3) será fundamento para delinear o escopo de aplicação do direito de explicação (tópico 5) e para identificar os limites desse direito para garantia da autodeterminação informativa do titular (tópico 6).

2. AS DECISÕES AUTOMATIZADAS BASEADAS EM DADOS PESSOAIS

O aumento na capacidade de processamento computacional e no armazenamento de dados, o volume expressivo de dados coletados por dispositivos conectados na internet, e o avanço na mineração e na análise massiva desses dados foram alguns dos elementos que culminaram na instauração de um contexto de *big data*. Esses elementos permitiram inovação na forma de processar dados, automatizar processos, extrair informações, obter *insights* a partir dos dados e tomar decisões. Com mais informações à disposição de empresas e governos, esses passaram a poder escolher sobre suas estratégias, políticas, sistemas e processos de maneira mais informada e consciente quanto às possibilidades e aos riscos envolvidos.

Apesar de terem sido utilizados como sinônimos nesta pesquisa, este contexto de *big data* evidencia uma pequena diferença conceitual entre dados e informação. Segundo Veronese, os dados passam a ter uma capacidade expressiva de se tornarem informações juridicamente relevantes diante do desenvolvimento do poder computacional¹³. Essa diferenciação demonstra a centralidade de uma proteção aos dados e não apenas às informações pessoais. Essa ideia também é trabalhada por Bruno Bioni, o qual afirma ser dado “o estado primitivo da informação, pois não é algo per se que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação”¹⁴. Dessa forma, *big data* é fenômeno resultado de um conglomerado de dados, ao passo que, a partir do seu processamento, podem ser extraídas informações, pessoais ou não.

¹³ VERONESE, Alexandre. Capítulo 14. Os direitos de explicação e de oposição diante das decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 1.

¹⁴ BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 31.

Associado ao *big data*, ferramentas de IA também proporcionaram um novo cenário para o processo de tomada de decisão. Essas permitem processar dados relevantes para formular uma decisão específica, identificar as perguntas pertinentes ou tópicos de atenção para os responsáveis, além de recomendar e prestar assistência aos interessados¹⁵. Com técnicas de IA, a análise de dados em um contexto de *big data* é potencializada pela capacidade de processar dados nos mais diversos padrões de tamanho, forma, extensão e linguagem.

Ferramentas de IA funcionam como uma chave para destravar o valor e as informações contidas no *big data*¹⁶. O processo de escolha e tomada de decisão, seja por pessoas físicas, seja por empresas, governos ou outras entidades, é expressivamente alterado. A finalidade dessa mudança é aprimorar esse processo em benefício dos interesses daqueles que tomam a decisão, agora baseada em dados, inclusive pessoais. Nesse tópico (tópico 2), será explorado de que forma a IA e os dados pessoais são utilizados nos processos de tomada de decisão, que passam a ser automatizados (tópico 2.1), bem como os conceitos básicos (tópico 2.2) e os casos de decisões automatizadas (tópico 2.3) para visualizar qual tipo de contexto a LGPD se refere quando regula o tema e os riscos à proteção de dados já identificados (tópico 2.4).

2.1. O impacto da Inteligência Artificial na tomada de decisão

As decisões automatizadas objeto desta pesquisa são aquelas resultado de processamentos massivos de dados pessoais a partir de algoritmos desenvolvidos para fazer a melhor escolha segundo os interesses programados. Um algoritmo nada mais é que um procedimento computacional para transformação de um valor de entrada em um valor de saída, o que pode ser aplicado para resolver problemas específicos¹⁷. Para que o sistema alcance um resultado adequado, ele utiliza diversos dados disponíveis, é neste ponto que o *big data* encontra sua relevância para o desenvolvimento da IA. Avanços no poder computacional e a criação da *World Wide Web* fizeram com que o *big data* facilitasse a criação de conjuntos de dados volumosos, que incluem incontáveis palavras de texto, imagens e horas de fala e

¹⁵ REINO UNIDO. Government Office for Science. **Artificial intelligence: opportunities and implications for the future of decision making**. 2016, p. 10. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf. Acesso em: 19 dez. 2022.

¹⁶ REINO UNIDO. Information Commissioner's Office. **Big data, artificial intelligence, machine learning and data protection**. 2017, p. 8 Disponível em: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Acesso em: 19 dez. 2022.

¹⁷ CORMEN, Thomas H. et al. **Introduction to algorithms**. 3. ed. Cambridge: The MIT Press, 2009, p. 5.

vídeo, bem como grandes quantidades de dados genômicos, de rastreamento de veículos, *clickstream*, redes sociais, entre outros¹⁸.

Não há consenso sobre o que seria IA ou se seria possível afirmar a existência de uma inteligência artificial. Alguns autores entendem que a inteligência artificial não é inteligente, ou seja, os sistemas de IA não são autônomos, racionais, ou capazes de discernir sem um treinamento amplo e computacionalmente intensivo com grandes conjuntos de dados ou regras e recompensas pré-definidas. Nesse sentido, a capacidade do computador depende do trabalho do humano. Um ponto de atenção é sobre o conceito de inteligência. Segundo Crawford, a inteligência não existe independentemente, como se fosse natural e distinta das forças sociais, culturais, históricas e políticas. Para a autora, na verdade, o conceito de inteligência tem causado danos excessivos ao longo dos séculos e tem sido usado para justificar relações de domínio desde a escravidão até a eugenia¹⁹.

A Comissão Europeia definiu IA como sistema de *software* (e possivelmente *hardware*) que, dado um objetivo complexo, atua na dimensão física ou virtual, percebendo seu ambiente através da aquisição de dados. Ainda, o sistema interpreta os dados estruturados ou não, raciocina (*reasoning*) sobre o conhecimento, processa as informações, derivadas destes dados, e decide a(s) melhor(es) ação(ões) a ser(em) tomada(s) para alcançar o objetivo dado, podendo inclusive alterar o ambiente²⁰.

Nesse sentido, Russell e Norvig destacam que “os filósofos tornaram a IA concebível ao sugerir que a mente é, de certa forma, como uma máquina, que opera sobre o conhecimento codificado em algumas linguagens, e esse pensamento pode ser usado para escolher as ações a serem tomadas”²¹. Em um primeiro momento, IA seria um sistema que se comporta de maneira inteligente enquanto racional (*rational IA system*). Esta é a habilidade da máquina escolher a melhor ação para se atingir um objetivo em acordo com (i) os critérios especificados por seu programador e (ii) os recursos disponíveis naquele ambiente. Para Russel e Norvig, essa forma de se identificar “a melhor decisão” guarda origem em conceitos

¹⁸ RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: a modern approach**. 4. ed. Reino Unido: Pearson, 2022, p. 44.

¹⁹ CRAWFORD, Kate. **Atlas of AI: Poder, Politics and the Planetary Costs of Artificial Intelligence**. New Haven: Yale University Press, 2021, p. 5 e 69.

²⁰ UNIÃO EUROPEIA. Comissão Europeia. **A definition of Artificial Intelligence: main capabilities and scientific disciplines**. High-Level Expert Group on Artificial Intelligence. 2019, p. 6. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Acesso em: 20 dez. 2022.

²¹ RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: a modern approach**. 4. ed. Reino Unido: Pearson, 2022, p. 52.

econômicos. Os economistas formalizaram o problema de tomar decisões para identificação de resultados que maximizem a utilidade esperada pelo tomador de decisão²².

Para que um sistema seja considerado inteligente, ele deve se subsumir ao conceito de agente racional. Um agente é aquele que percebe seu ambiente através de sensores e age sobre esse ambiente através de atuadores (*actuators*)²³. Um ambiente é um espaço físico ou virtual cujo estado é levado em consideração quando o agente é desenvolvido. Ou seja, a parte afeta o que o agente percebe e é afetada pelas ações do agente. Nesse sentido, um agente racional atua de forma a maximizar o valor esperado da medida de desempenho, considerando o ambiente e os dados percebidos nele até um momento específico.

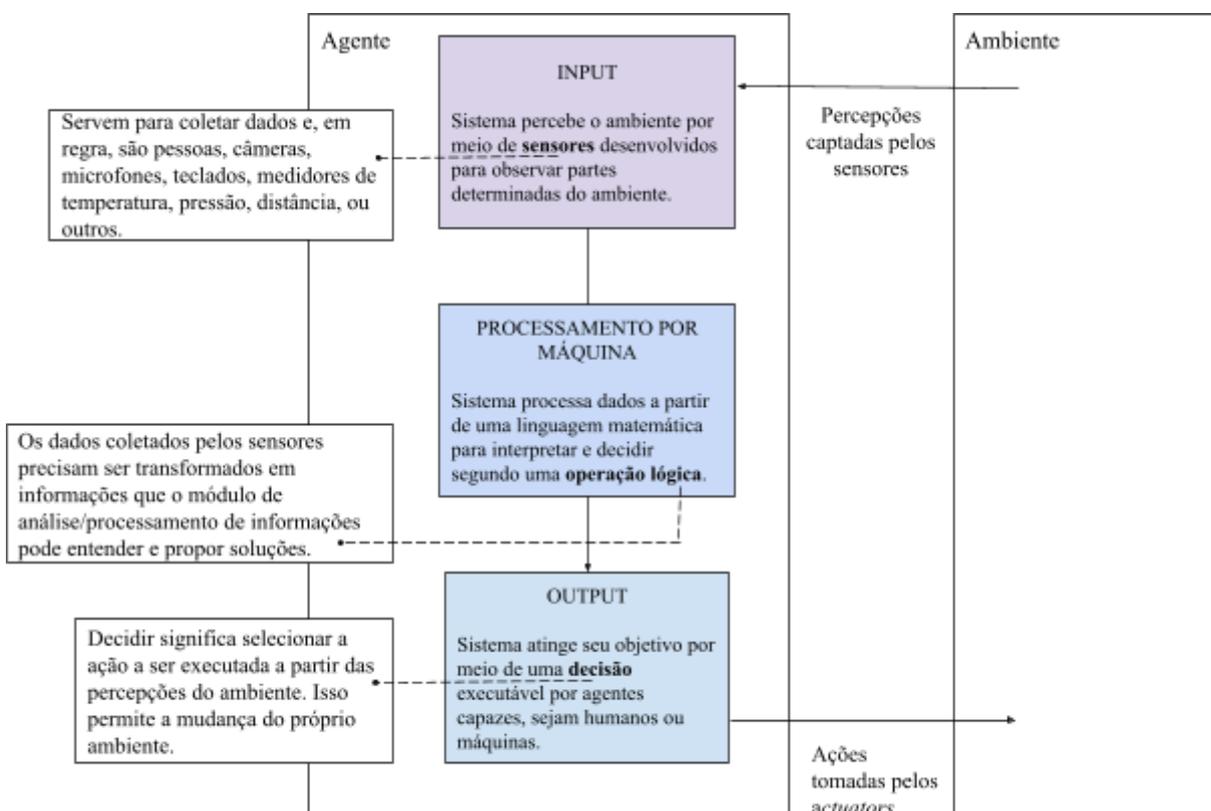


Figura 1 - Fluxograma do funcionamento de sistemas de IA²⁴

²² RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: a modern approach**. 4. ed. Reino Unido: Pearson, 2022, p. 52.

²³ RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: a modern approach**. 4. ed. Reino Unido: Pearson, 2022, p. 5.

²⁴ Para a elaboração desse fluxograma, foram usados como base os modelos da UNIÃO EUROPEIA. Comissão Europeia. **A definition of Artificial Intelligence: main capabilities and scientific disciplines**. High-Level Expert Group on Artificial Intelligence. 2019, p. 2. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Acesso em: 20 dez. 2022. e OCDE. **Artificial Intelligence**. Paris: OECD Publishing, 2019. 1. The technical landscape. Disponível em: https://www.oecd-ilibrary.org/sites/eedfee77-en/1/2/1/index.html?itemId=/content/publication/eedfee77-en&_csp=5c39a73676a331d76fa56f36ff0d4aca&itemIGO=oecd&itemContentType=book Acesso em: 21 dez. 2022.

Em acordo com esse fluxograma sobre os sistemas de IA, o processo de tomada de decisão com base em informações é feito quando um agente humano ou não, em determinado período de tempo, observa um ambiente por meio de sensores específicos, o que pode tornar a observação incompleta ou ruidosa. A partir do que foi percebido, o agente escolhe uma ação como sendo sua decisão final a ser tomada. Porém, quando esse modelo é levado para sistemas automatizados, alguns aspectos de imprecisão são adicionados: (i) incerteza sobre os resultados (*outputs*), em que os efeitos das ações escolhidas são incertos; (ii) incerteza do modelo, no qual o modelo de descrição do problema é incerto; (iii) incerteza do estado, em que o verdadeiro estado e condição do ambiente é incerto; e (iv) incerteza da interação, quando o comportamento dos outros agentes que interagem no ambiente é incerto.

Em regra, são em cenários como esses que decisões são tomadas e estes são os aspectos determinantes para o resultado final: possibilidades e efeitos dos outputs, modelos de descrição do problema, características do ambiente e interações entre os agentes²⁵. Para enfrentar esse cenário, alguns métodos são utilizados, como a programação explícita, que consiste em antecipar todos os cenários possíveis e programar explicitamente o que o agente deve fazer em resposta a cada um deles, esse método seria o adequado para solução de problemas simples, nos quais é possível mapear todas as possibilidades²⁶.

O último passo é decidir qual ação tomar. Em regra, a fundamentação/decisão que faz parte de um sistema de IA é complexo, por isso requer-se uma combinação de várias das técnicas acima mencionadas²⁷. Ainda, os sistemas de IA não são estanques. Mas devem ser aprimorados de forma constante por meio de verificação e validação dos modelos, monitoramento do seu impacto, avaliação da conformidade com regulamentação, de mudanças organizacionais e da experiência do usuário, bem como a revisão dos dados coletados e processados pelo sistema²⁸. Ter visibilidade sobre os elementos considerados

²⁵ KOCHENDERFER, Mykel; WHEELER, Tim; WRAY, Kyle. **Algorithm for Decision Making**. Massachusetts: The MIT Press, 2022, p. 2. Disponível em: <https://algorithmsbook.com/files/dm.pdf>. Acesso em: 21 dez. 2022.

²⁶ KOCHENDERFER, Mykel; WHEELER, Tim; WRAY, Kyle. **Algorithm for Decision Making**. Massachusetts: The MIT Press, 2022, p. 6. Disponível em: <https://algorithmsbook.com/files/dm.pdf>. Acesso em: 21 dez. 2022.

²⁷ DONEDA, Danilo et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018. Disponível em: <https://ojs.unifor.br/rpen/article/view/8257/pdf>. Acesso em: 20 dez. 2022. UNIÃO EUROPEIA. Comissão Europeia. **A definition of Artificial Intelligence: main capabilities and scientific disciplines**. High-Level Expert Group on Artificial Intelligence. 2019, p. 36. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Acesso em: 20 dez. 2022.

²⁸ OCDE. **Artificial Intelligence**. Paris: OECD Publishing, 2019. 1. The technical landscape. Disponível em: https://www.oecd-ilibrary.org/sites/eedfee77-en/1/2/1/index.html?itemId=/content/publication/eedfee77-en&_csp=5c39a73676a331d76fa56f36ff0d4aca&itemIGO=oecd&itemContentType=book Acesso em: 21 dez. 2022.

pelos sistemas para a tomada de decisão, bem como os espaços de incerteza, é relevante para que se compreenda de que forma a decisão final é escolhida. Isso influencia em quais cenários seria possível explicar o processo.

Esse processo é ainda mais complexo em contextos em que a “inteligência” da IA não se restringe à racionalidade, mas também considera a capacidade de aprendizado do sistema a partir de experiências (*IA learning rational system*). Os sistemas de aprendizado de máquinas (*machine learning*) são resultados desse sistema e são um dos métodos de desenvolvimento de IA mais relevantes atualmente, diante de sua capacidade de solucionar problemas que não foram precisamente especificados anteriormente, ampliando a sua usabilidade em atividades cotidianas²⁹.

O aprendizado de máquinas, em regra, pode ser treinado e aprimorado de três formas: (i) aprendizado supervisionado; (ii) não supervisionado; e (iii) por reforço, como evidenciado na tabela a seguir.

	Supervisionado	Não supervisionado	Por reforço
F U N C I O N A M E N T O	Quando o sistema é exposto a exemplos de entradas e saídas já conhecidas que formam uma base de dados identificados (label) para treinamento . A partir dessa base, o sistema realiza conexões, percebe padrões e descreve essas relações de forma adequada para identificação de novas entradas. É necessária uma base inclusiva e diversa para treinamento e validação do modelo. O treinamento do sistema é realizado pela minimização da função de	O sistema desenvolve e organiza os dados de acordo com uma lógica não conhecida ou definida <i>a priori (unlabel)</i> . Para tanto, o sistema identifica padrões e relações “escondidas” entre os dados de forma agrupá-los em aglomerados não definidos anteriormente. Aprendizagem sem supervisão é aprender pela lógica de identificar padrões ocultos em um conjunto de dados não identificado.	Um agente percebe o ambiente em que foi exposto e aprende a tomar decisões para maximizar a recompensa a longo prazo a partir da aprovação de uma experiência . O agente inicia o processo de busca pela maior recompensa sem dados identificados ou direcionamento na ação que deve tomar. Como ele tem poder de agir, ele precisa manter um equilíbrio entre a exploração de possíveis ações, realizando uma variedade de decisões

²⁹UNIÃO EUROPEIA. Comissão Europeia. **A definition of Artificial Intelligence: main capabilities and scientific disciplines**. High-Level Expert Group on Artificial Intelligence. 2019, p. 3. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Acesso em: 20 dez. 2022. Para além das aplicações de aprendizado de máquina, a IA é base para ferramentas de visão computacional, processamento de linguagem natural e outros. GREGGARD, Samuel. **What is Artificial Intelligence & How Does It Work?** 2019. Disponível em: <https://www.datamation.com/artificial-intelligence/what-is-artificial-intelligence>. Acesso em: 27 jan. 2023.

	custo que representa a ligação entre a entrada e a saída desejada ³⁰ .		usando tentativa e erro para favorecer as ações que produzem a recompensa máxima.
O B J E T I V O	Prever os resultados para novos dados pertencentes ao mesmo domínio que os dados de entrada. O modelo não deve ser aplicado a um domínio de dados diferente. O sistema aprende apenas um tipo de tarefa com base no conjunto de dados identificados.	Obter <i>insights</i> , identificar padrões e conexões a partir dos dados não identificados que podem prever se os novos dados fazem parte do grupo ou se são uma anomalia.	Aprender sequências de ações através da exploração de possibilidades em um ambiente para maximizar recompensas. Esse método pode lidar com um cenário inteiramente novo.

Figura 2 - Tabela das formas de aprendizado em *machine learning*³¹

A definição desses métodos de aprendizado de máquinas e a operação lógica de um sistema de IA em um conceito tradicional são relevantes para entender os efeitos das decisões automatizadas na sociedade. Isso porque uma decisão tomada com base em dados categorizados (*labeled data*) e elementos (*features*) pré-calculados permite a identificação de quais elementos foram levados em consideração para a decisão final. Os outros modelos tornam essa visibilidade mais dificultosa e não direta, já que permite que o próprio sistema perceba padrões a serem repetidos. A precisão de um modelo é facilmente verificada em sistemas que se utilizaram de dados de entrada categorizados³². Para além dessas três formas, a aprendizagem semi supervisionada utiliza de forma combinada uma porção de dados categorizados e não categorizados dos quais o modelo deve aprender e fazer previsões sobre novos exemplos. Essa forma é relevante em cenários que existem poucos dados categorizados e isso geraria esforços significativos de recursos financeiros e tempo³³.

O desenvolvimento das ferramentas de aprendizagem de máquina avançaram para uma nova forma de aprendizagem ainda mais complexa e indireta chamada aprendizado profundo de máquinas (*deep learning*). Esse sistema é uma forma de aprendizado de

³⁰ MASOLO, Claudio. **Supervised, unsupervised and deep learning**. 2017. Disponível em: <https://towardsdatascience.com/supervised-unsupervised-and-deep-learning-aa61a0e5471c>. Acesso em: 21 dez. 2022.

³¹ KHANDELWAL, Renu. **Supervised, Unsupervised, and Reinforcement Learning**. 2019. Disponível em: <https://arshren.medium.com/supervised-unsupervised-and-reinforcement-learning-245b59709f68>. Acesso em: 21 dez. 2022.

³² DINAMARCA. Datatilsynet. **Artificial intelligence and privacy**. 2018. Disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Acesso em: 06 fev. 2023, p. 9.

³³ BROWNLEE, Jason. **What is semi-supervised learning**. 2021. Disponível em: <https://machinelearningmastery.com/what-is-semi-supervised-learning/>. Acesso em: 06 fev. 2023.

máquinas que busca simular os mesmos princípios da rede neural (*neural networks*) do cérebro humano. Sistemas desse tipo geralmente são baseados em um conjunto conhecido de dados de treinamento que ajudam os algoritmos a realizar uma tarefa. Esse funcionamento depende da própria rede ser capaz de determinar a resposta correta para se chegar no objetivo desejado³⁴. Dessa forma, o resultado final de uma decisão tomada com base em redes neurais é determinado por uma série de elementos que compõem camadas de decisão não determinadas por humanos, mas foram calculados e ajustados durante o processo de treinamento do modelo para se alcançar o objetivo final³⁵. Para sistematizar os conceitos de IA, *machine learning* e *deep learning*, o seguinte quadro pode ser formulado:

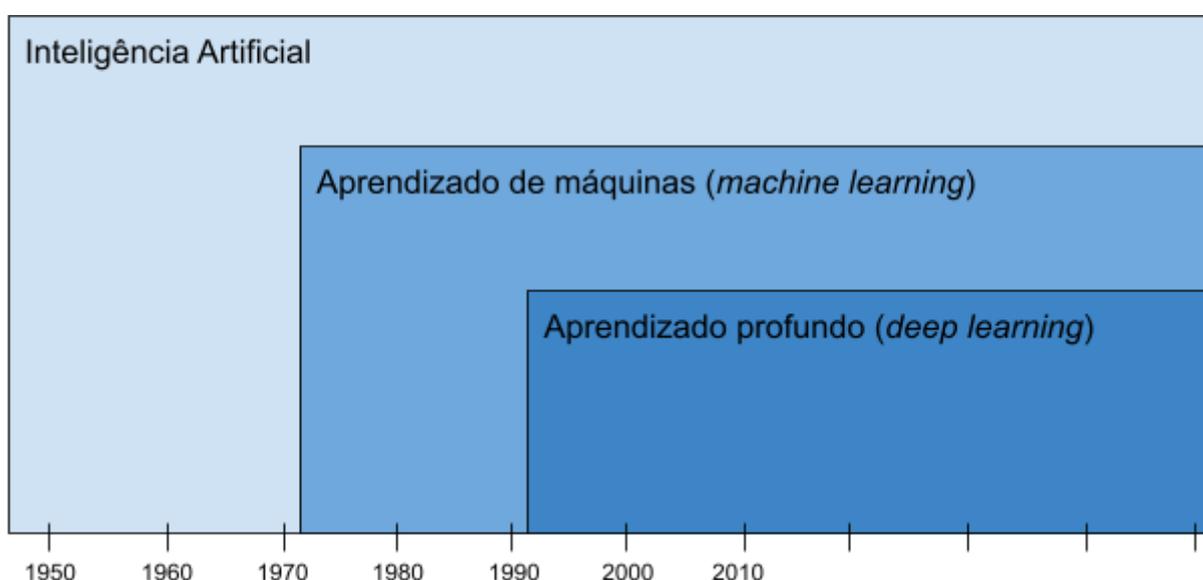


Figura 3 - Quadro sobre a relação entre IA, *machine learning* e *deep learning*³⁶

Os algoritmos de IA não seriam apenas códigos matemáticos que podem decidir sobre acesso a benefícios, serviços e produtos. Eles são mecanismos construídos e geridos institucionalmente e socialmente para assegurar uma lógica específica de conhecimento. Isso ocorre por meio de padrões de inclusão ou exclusão de pessoas e dados, antecipação de fenômenos, avaliação da relevância de certos fatos de forma personalizada, inclusive em uma perspectiva social de grupos³⁷. A tomada de decisão automatizada, como a definição de perfis,

³⁴ DINAMARCA. Datatilsynet. **Artificial intelligence and privacy**. 2018. Disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Acesso em: 06 fev. 2023, p. 6.

³⁵ DINAMARCA. Datatilsynet. **Artificial intelligence and privacy**. 2018. Disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Acesso em: 06 fev. 2023, p. 14.

³⁶ KOZYRKOV, Cassie. **Are you using the term AI incorrectly?** 2018. Disponível em: <https://hackernoon.com/are-you-using-the-term-ai-incorrectly-911ac23ab4f5>. Acesso em: 06 fev. 2023.

³⁷ GILLESPIE, Tarleton. The Relevance of Algorithms. In: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo; FOOT, Kirsten. **Media Technologies**. Cambridge: MIT Press, 2013, p. 3.

pode levar, em uma primeira análise, a decisões mais rápidas e mais consistentes³⁸. Porém, há riscos significativos para os indivíduos. Será em vista desse pressuposto que a regulação avança para traçar obrigações aos agentes que utilizam dados pessoais para tomar decisões automatizadas.

2.2. Decisões automatizadas reguladas pela LGPD

O desenvolvimento da técnica e dos recursos necessários para disseminação de sistemas de IA deixou rastros na regulação de proteção de dados. Muitas dessas ferramentas funcionam a partir do tratamento de dados pessoais e já há impactos explícitos no campo dos direitos dos titulares de dados. De forma geral, essas normas versam sobre a possibilidade e as salvaguardas relacionadas a decisões tomadas com base em dados pessoais por meios automatizados que afetam significativamente os direitos e interesses das pessoas.

No Brasil, o tema é regulado pelo art. 20, da LGPD, que delimita seu âmbito de aplicação especificamente às decisões baseadas unicamente no tratamento automatizado de dados pessoais as quais afetem seus interesses. Esse conceito inclui as decisões destinadas a definir o perfil pessoal, profissional, de consumo e de crédito ou os aspectos de personalidade do titular. Sendo assim, as decisões objeto de regulação pela LGPD são: (i) decisões automatizadas, ou seja, sem interferência humana; (ii) com base em dados pessoais; e (iii) que afetem os interesses dos titulares

Em vista dos documentos do Grupo de Trabalho do Art. 29 e do *Information Commissioner's Office*, uma decisão que atende o primeiro elemento não sofre interferência relevante por um humano. Esses estudos focam na condicionante de não participação humana, explícita no termo “unicamente”, e não na definição do que seria um tratamento automatizado. Ainda nesse contexto, uma decisão que atende o terceiro elemento é aquela que produz algum efeito jurídico, econômico ou social para o titular³⁹.

³⁸ ARAUJO, Theo et al. In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & Society*, v. 35, p. 611–623, 2020, p. 614.

³⁹ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. 2017, p. 10. Disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963. Acesso em: 14 dez. 2022. REINO UNIDO. Information Commissioner's Office. **Rights related to automated decision making including profiling**. [s.d]. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>. Acesso em: 11 nov. 2022.

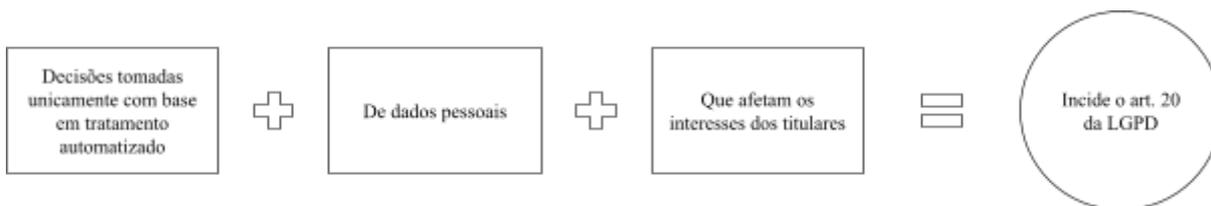


Figura 4 - Conceito de decisão automatizada na LGPD

Ainda não há definição de parâmetros mais concretos sobre o que seria ou não considerada decisão automatizada no escopo do art. 20. Diante disso, a ANPD já indicou intenção em apresentar diretrizes sobre o tema de IA durante os anos de 2023 e 2024, em vista também dos seus influxos na proteção de dados e a vulnerabilidade do titular⁴⁰. Para sanar essa indeterminação, está em tramitação no Senado Federal o Projeto de Lei (PL) 4496, de 2019, que visa alterar a LGPD para dispor de forma específica sobre o conceito de decisões automatizadas enquanto qualquer processo o qual utilize técnica computacional para escolher, classificar, aprovar ou rejeitar, atribuir medida, cálculo de risco ou de probabilidade.

Segundo o PL, decisão automatizada é “processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou escore, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais [...]”. O PL não define decisão automatizada por não ter participação significativa de pessoas. Uma alteração legislativa nesse sentido poderia trazer maior segurança para a definição do que é ou não uma decisão automatizada. Porém, corre-se o risco dessa redação ser suplantada rapidamente pelo avanço tecnológico que poderá desenvolver novas atividades não descritas no texto do PL⁴¹. Apesar dessa possível lacuna no Brasil, o tema de decisão automatizada foi regulamentado por outras normas jurídicas de proteção de dados, de forma que outras autoridades já se debruçaram pelo tema, como o exemplo da UE.

O art. 22 do RGPD, com um texto bastante similar ao da LGPD, regula decisões baseadas exclusivamente no tratamento automatizado que afetam a esfera jurídica ou de forma significativa o titular. O Grupo de Trabalho do Art. 29 já evidenciou que estão no escopo deste conceito as decisões que não possuem um humano envolvido de forma efetiva no processo. Ou seja, seria uma decisão baseada exclusivamente no processamento

⁴⁰ A Agenda Regulatória para o biênio 2023-2024 foi publicada como anexo da Portaria ANPD nº 35, de 4 de novembro de 2022. BRASIL. **Portaria ANPD nº 35, de 4 de novembro de 2022**. 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885>. Acesso em: 12 dez. 2022.

⁴¹ O projeto foi apresentado em 2019 e será analisado pelas Comissões de Ciência, Tecnologia, Inovação, Comunicação e Informática e de Constituição, Justiça e Cidadania, que deliberará de forma terminativa. No entanto, o projeto está aguardando a designação de relator desde fevereiro de 2021. Para mais informações, acesse: <https://www25.senado.leg.br/web/atividade/materias/-/materia/138136>.

automatizado o caso de uma pessoa, que não tem autoridade ou competência para mudar a decisão, aplicar rotineiramente perfis gerados automaticamente a indivíduos sem nenhuma influência sobre o resultado. Além disso, a esfera jurídica do titular seria impactada quando a decisão: (i) permitir ou negar um determinado benefício social concedido por lei; (ii) limitar sua liberdade de ir e vir e se associar, como a recusa da entrada de uma pessoa na fronteira, ou sujeitá-la a medidas de segurança ou vigilância acrescida pelas autoridades competentes; ou (iii) alterar seus direitos ou estado legal em um contrato, como desconectar automaticamente o serviço de telefonia móvel por quebra de contrato, porque se esqueceu de pagar sua conta⁴².

De forma complementar, o RGPD se aplica sempre que a decisão tiver o potencial de influenciar significativamente as circunstâncias, o comportamento ou as escolhas das pessoas envolvidas. Como exemplo, o Grupo de Trabalho destaca os casos de aceite ou de recusa automática de pedido de crédito on-line, de práticas de recrutamento eletrônico sem qualquer intervenção humana, ou de publicidade direcionada, dependendo (i) da intrusividade do processo de elaboração do perfil; (ii) das expectativas e desejos das pessoas envolvidas; (iii) da forma como o anúncio é entregue; e (iv) das vulnerabilidades particulares das pessoas visadas. Outro exemplo seria caso de definição de preços de forma automatizada que resulta em preços diferentes para agentes diferentes quando os preços forem expressivamente altos e, por isso, barrarem efetivamente alguém de acessar certos bens ou serviços⁴³. Esses parâmetros ainda não foram definidos no contexto brasileiro.

Os termos utilizados para caracterizar uma decisão automatizada como aquela que interfere significativamente a esfera de direitos do titular são circunstanciais, de forma que a análise da relevância da decisão automatizada deve ser caso a caso. Em 2021, o Tribunal de Justiça de Amsterdam, *Rechtbank Amsterdam*, julgou o caso C/13/687315 / HA RK 20-207⁴⁴ sobre a pertinência de uma decisão automatizada, caso que traz parâmetros iniciais sobre a incidência ou não da regulação na decisão automatizada com base em dados pessoais. No caso, a empresa Uber foi processada por uma associação de motoristas de aplicativo por, dentre outras questões, estar utilizando ferramentas de decisão automatizada sem a devida

⁴² UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 21. Disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963. Acesso em: 14 dez. 2021.

⁴³ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 22. Disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963. Acesso em: 14 dez. 2021.

⁴⁴ PAÍSES BAIXOS. Rechtbank Amsterdam. C/13/687315 / HA RK 20-207. Julgado em 11.03.2021. Disponível em: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/687315_/HA_RK_20-207. Acesso em: 26 dez. 2022.

informação ao titular. O Tribunal entendeu que o sistema da Uber de pareamento do passageiro com o motorista mais próximo e de precificação das corridas não seria uma decisão significativa para a esfera de direitos do titular, apesar de serem decisões que afetam o desempenho do contrato entre o Uber e o motorista. Em outro caso, C/13/692003/HA RK 20-302⁴⁵, o mesmo tribunal analisou a decisão tomada automaticamente de bloquear temporariamente o acesso ao aplicativo a um motorista após um sinal de fraude, sem intervenção humana. Para a Corte, esse bloqueio temporário não teve nenhum efeito duradouro ou permanente, de modo que a decisão automatizada não teve consequências legais ou afetou significativamente o motorista.

Apesar das semelhanças, as normas de proteção de dados brasileira e europeia enunciam uma regulação sobre decisão automatizada para finalidades diferentes: o art. 22(1) do RGPD proíbe, em regra, que um titular de dados seja submetido a decisões automatizadas que o afetem significativamente. As exceções a essa regra ocorrem quando a decisão (i) for necessária para a celebração ou a execução de um contrato entre o titular e o controlador; (ii) for autorizada por lei do país no qual o controlador estiver sujeito, e essa lei prever medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou (iii) for baseada no consentimento explícito do titular dos dados⁴⁶.

O documento do Grupo de Trabalho destaca que a exceção da execução de contrato deve ser interpretada de forma restritiva. Essa não é a base legal para o tratamento automatizado de dados nos casos de lojas on-line não podem argumentar que a definição de perfis, profiling, é necessária para compras on-line, mesmo quando o perfil é mencionado no contrato escrito. Essa base se aplica nos casos de uso de decisões automatizadas para: (i) potencialmente permitir maior consistência ou justiça no processo de tomada de decisões (por exemplo, reduzindo o potencial de erro humano, discriminação e abuso de poder); (ii) reduzir o risco de os clientes não cumprirem com os pagamentos de bens ou serviços (por exemplo,

⁴⁵ PAÍSES BAIXOS. Rechtbank Amsterdam. C/13/692003/HA RK 20-302. Julgado em: 11.03.2021. Disponível em: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/692003/HA_RK_20-302. Acesso em: 26 dez. 2022.

⁴⁶ Para mais informações dos requisitos previstos no RGPD para tomada de decisão automatizada baseada em dados pessoais e com efeitos significativos para os interesses dos titulares, leia: MENDOZA, Isak; BYGRAVE, Lee. The Right not to be Subject to Automated Decisions based on Profiling. In: SYNODINOU, Tatiani *et al.* (eds.). **EU Internet Law: Regulation and Enforcement**. [s.l.]: Springer, 2017. ROIG, Antoni, Safeguards for the right not to be subject to a decision based solely on automated processing (Article22 GDPR). **European Journal of Law and Technology**, v. 8, n. 3, 2017.

utilizando o referenciamento de crédito); ou (iii) permitir que tomem decisões em um prazo mais curto e melhorem a eficiência⁴⁷.

Segundo o art. 22(3), quando as exceções (i) e (iii) forem aplicáveis, cabe ao controlador adotar medidas adequadas para salvaguardar os direitos, liberdades e legítimos interesses do titular dos dados, o que inclui, no mínimo, o direito de intervenção humana no processo decisório, o direito do titular se manifestar e contestar a decisão. O Grupo de Trabalho destaca que a necessidade de salvaguardas no uso de decisão automatizada enfatiza o princípio da transparência, já que o titular só poderá contestar uma decisão ou expressar sua opinião se entender completamente como e em que base ela foi tomada. Os controladores devem realizar avaliações frequentes sobre os conjuntos de dados que processam para verificar qualquer viés, e desenvolver maneiras de tratar qualquer elemento prejudicial, incluindo qualquer dependência excessiva em correlações. Sistemas que auditam algoritmos e revisões regulares da precisão e relevância da tomada de decisão automatizada, incluindo a definição de perfis, são outras medidas úteis⁴⁸.

Já o art. 20 da LGPD destaca as decisões automatizadas para apresentar um direito de revisão e de informação sobre os critérios e procedimentos utilizados, como consequência o fundamento legal que autoriza o tratamento de dados em decisões automatizadas são os mesmos aplicáveis aos outros tratamentos especificados nos art. 7º e 11, quando o objeto for dado pessoal sensível.

Há convergência entre os conceitos de decisões automatizadas relevantes reguladas pelas normas de proteção de dados brasileira e europeia, as duas se ocupam de decisões sem intervenção humana fundamentadas em dados pessoais e com impacto relevante para o titular, apesar da flexibilidade do que significa esse impacto relevante. Destaca-se que as obrigações específicas às decisões automatizadas apenas são aplicáveis quando a decisão é tomada pelo sistema e este não apenas apoia a decisão final, nestes casos haveria uma participação relevante do humano. Como será analisado nesta pesquisa (tópico 5.2.2 e 5.2.3), esse mesmo conceito se repete na norma de proteção de dados do Uruguai, por outro lado, a Colômbia não apresenta uma definição para o que seria decisões automatizadas reguladas pela lei.

Por fim, ainda na definição de um conceito de decisão automatizada, é importante dar um passo atrás e pontuar que sistemas de IA são diferentes de simples sistemas

⁴⁷ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. 2017, p. 14. Disponível em: <https://ec.europa.eu/newsroom/article29/redirect/document/49826>. Acesso em: 08 dez. 2022.

⁴⁸ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. 2017, p. 17. Disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963. Acesso em: 14 dez. 2021.

automatizados. Técnicas de automação são utilizadas desde a primeira revolução industrial, quando era possível que máquinas se movessem sem intervenção humana. A automação ocorre quando um *hardware* ou *software* é capaz de realizar tarefas automaticamente, sem intervenção humana, normalmente essas atividades são repetitivas e monótonas, sem que seja necessária reflexão sobre o resultado. Em caso de simples automação, é possível prever facilmente o resultado de saída, de acordo com as ordens dadas e as informações de entrada. A título exemplificativo, não há indícios que o governo federal tenha utilizado sistemas de IA para definição de quais pessoas estariam aptas a receber o Auxílio Emergencial, porém é lógico perceber o uso de soluções de automação para a padronização de deferimentos ou indeferimentos sem ser necessário a análise individual do solicitante⁴⁹. Já, no caso de IA, há relativa incerteza sobre o resultado, os dados ganham centralidade, e há a capacidade de aprender com os resultados, esses são requisitos para que a ferramenta funcione devidamente⁵⁰. Assim, nem todo sistema automatizado é um sistema de IA, mas o conceito de decisão automatizada abarca tanto sistemas automatizados quanto sistemas de IA. Devido a complexidade de ferramentas de IA, esta pesquisa se debruçará de forma mais detida sobre as decisões automatizadas baseadas em IA e consequente explicabilidade referente a elas.

2.3. Casos concretos de decisões automatizadas reguladas pela LGPD

Decisões automatizadas baseadas em dados pessoais com efeitos para os interesses dos titulares são utilizadas em diversos contextos. Um dos principais usos de IA nesse sentido ocorre em sistemas anti-fraude e de segurança da informação no sistema bancário. Um exemplo é o uso de fotos de perfil de clientes de bancos para comparar com as fotos de documentos pessoais desses usuários por meio da tecnologia de reconhecimento facial automatizado, validar a identidade e, com isso, permitir a abertura de uma conta ou uma transação financeira. Caso a verificação por meio dos dados da face do usuário falhe e o sistema indique caso de fraude, o cliente pode ser impedido ou ter processo de criação de conta bancária dificultado. Ferramentas para detecção de transações eletrônicas fraudulentas também são resultado de decisões automatizadas que percebem a quebra de padrão de consumo do usuário por meio, por exemplo, do horário de compra de um produto, o valor

⁴⁹ TAVARES, Clarice *et al.* **O Auxílio Emergencial no Brasil: Desafios na implementação de uma política de proteção social datificada.** 2022. p. 21. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/01_Informe-Brasil_Inteligencia-Artificial-e-Inclusao_PT_22042022.pdf. Acesso em: 15 dez. 2022.

⁵⁰ HANKIEWICZ, Kamila. **What Is The Real Difference Between Automation And AI?** 2018. Disponível em: <https://becominghuman.ai/what-is-the-real-difference-between-automation-and-ai-366513e0c910>. Acesso em: 12 dez. 2022.

desse produto, a localização da loja e o comportamento comum do cliente. Processos como esses já são utilizados pelo Banco do Brasil, Caixa Econômica Federal e Banco Nacional de Desenvolvimento Econômico e Social⁵¹.

No setor de seguros, dados pessoais também têm sido utilizados como insumo para desenvolvimento do produto, vendas e distribuição dos seguros, serviços de assistência, e precificação. Durante os processos de cotação e renovação de seguros, é calculado um *score* de forma automatizada para medir o risco ou probabilidade de que uma pessoa faça uma reclamação ou sofra uma perda, ou seja, utilize o seguro. Ter um *score* elevado implica no pagamento de um preço mais alto que outras pessoas com *score* baixo para o mesmo seguro contratado. No processo de precificação de seguros de saúde, em regra, os sistemas automatizados levam em consideração informações como as condições médicas no momento da contratação, idade do segurado, estilo de vida, profissão, e localização de residência⁵². Ter acesso aos serviços de seguro impacta de forma relevante o titular, já que esses serviços possuem repercussão transindividual e utilidade pública⁵³.

Já no mercado de crédito, as decisões automatizadas definem o *score* de crédito dos consumidores, que busca medir a capacidade de adimplemento da obrigação creditícia do consumidor frente às instituições financeiras, como os bancos e *bureau* de crédito. Nesse modelo, o sistema automatizado analisa os dados pessoais do consumidor, principalmente comportamentais disponíveis em contexto de *big data*, para prever seu comportamento futuro e, com isso, indicar a probabilidade dele cumprir ou não com suas obrigações, definindo a taxa de juros individualizada que seria cobrada pelo crédito concedido⁵⁴. Esses sistemas de análise de crédito por *score* disponíveis no Brasil são regulados pela LCP. Ela dispõe sobre 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. Esses sistemas, que geram *score* de forma automatizada, levam em consideração declaração de falência, perda de

⁵¹ TRANSPARÊNCIA BRASIL. **Uso de Inteligência Artificial pelo Poder Público. Recomendações de Governança**. 2020. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 26 dez. 2022.

⁵² UNIÃO EUROPEIA. European Insurance and Occupational Pensions Authority. **Big data analytics in motor and health insurance: a thematic review**. Luxembourg: Publications Office of the European Union, 2019, p. 36-38.

⁵³ GRAVINA, Maurício Salomoni. **Princípios Jurídicos do Contrato de Seguro**. Rio de Janeiro, Funenseg, 2015, p. 16.

⁵⁴ SOUZA, Maique Barbosa de. **Governança em bancos de dados de análise de crédito para instituições financeiras a partir do uso da inteligência artificial e das decisões automatizadas**: como a adequação interna pode contribuir para a correta definição do risco representado no score de crédito. Dissertação (mestrado) Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, Porto Alegre, 2022, p. 30

emprego, histórico de pagamentos atrasados, emprego formal, além de outros dados do consumidor e acabam por definir o acesso das pessoas a bens e serviços.

Outro caso que chama atenção é o uso de avaliações de usuários em aplicativos de prestação de serviço de transporte de produtos ou pessoas, como o Uber, Ifood, 99 e outros. Nesses casos, decisões automatizadas são feitas para gerar o *score* do prestador de serviço com base nas notas atribuídas pelos usuários do aplicativo e em outros parâmetros, como a geolocalização do prestador de serviço, nota atribuída pelo comerciante de produtos, pontuação determinada pela prestação de serviços em horas de alta demanda, pedidos efetivamente entregues, e pontuação determinada com base no número de pedidos propostos ao condutor.

A autoridade de proteção de dados italiana, julgando caso sobre a conformidade de um sistema como esse com RGPD, fixou entendimento de que essas decisões são classificadas como relevantes para os interesses do titular, já que esse *score* atribui a cada condutor uma pontuação que dá acesso prioritário ao sistema de seleção das faixas de horário com alta demanda estabelecido pela empresa, dentro do qual os pedidos recebidos são distribuídos diariamente, ou seja, o *score* é utilizado para restringir uma parte dos condutores das oportunidades de trabalho⁵⁵. Outro exemplo de decisão automatizada em aplicativos de entrega se refere à atribuição de pedidos dentro dos turnos reservados que processa pelo menos, de acordo com o que foi declarado, os dados relativos à posição geográfica e ao tipo de meio de transporte utilizado pelo condutor considerado em relação à posição do cliente e da empresa⁵⁶.

Como exemplificado, as decisões automatizadas são utilizadas para a definição de perfis, ou seja, a partir do tratamento de dados pessoais, aspectos da personalidade são avaliados, como desempenho profissional de uma pessoa, a sua situação económica, estado de saúde, preferências pessoais, interesses, comportamento, lugares que frequenta, entre outras aspectos. Outro setor que se utiliza dessa forma de processamento de dados é o do entretenimento, seja para moderação de conteúdo⁵⁷, como mencionado na introdução desta

⁵⁵ ITÁLIA. Garante per la Protezione dei Dati Personali. **9675440**. Julgado em: 10.06.2021. Disponível em: [https://gdprhub.eu/index.php?title=Garante per la protezione dei dati personali \(Italy\) - 9675440](https://gdprhub.eu/index.php?title=Garante+per+la+protezione+dei+dati+personali+(Italy)+-+9675440). Acesso em: 27 dez. 2022.

⁵⁶ ITÁLIA. Garante per la Protezione dei Dati Personali. **9685994**. Julgado em: 22.07.2021. Disponível em: [https://gdprhub.eu/index.php?title=Garante per la protezione dei dati personali \(Italy\) - 9685994](https://gdprhub.eu/index.php?title=Garante+per+la+protezione+dei+dati+personali+(Italy)+-+9685994). Acesso em: 27 dez. 2022. Esse caso foi julgado pela autoridade italiana de forma similar ao anterior.

⁵⁷ ARCEGAS, João Victor. **Proteção de Dados e Transparência em Moderação de Conteúdo na Europa, Reino Unido e Brasil**. 2021. Disponível em: <https://itsrio.org/wp-content/uploads/2021/07/Protecao-de-Dados-e-Transparencia-em-Moderacao-de-Conte%C3%BAdo.pdf>. Acesso em: 28 dez. 2022.

pesquisa (tópico 1), seja para anúncios publicitários personalizados ou recomendações de conteúdos ou produtos para consumo.

A publicidade online, associada a técnicas de IA, possui uma vantagem competitiva frente às práticas tradicionais de publicidade em meios de comunicação em massa por aumentar a precisão da segmentação de usuários a partir de dados pessoais contextuais ou explicitamente informados pelo usuário. Com a publicidade direcionada, os anunciantes podem ser mais específicos sobre o público-alvo que desejam impactar e os usuários passam a receber anúncios vinculados a seus interesses e preferências registradas *online*⁵⁸. Essa segmentação é, em regra, feita por decisões automatizadas, ou seja, é a máquina que percebe padrões nos usuários e os encaixa em perfis.

Um exemplo é quando um usuário busca determinado produto no navegador de seu celular e tempo depois um anúncio deste produto está nas páginas de suas redes sociais. As redes, em regra, conhecem o conteúdo que as pessoas estão postando, seus dados demográficos auto-relatados, a identidade de seus amigos, traços de navegação na web, entre outras informações pessoalmente identificáveis (*personally-identifiable information* - PII). Nesses casos, para além da perfilização feita por redes sociais com base em dados coletados nas redes, o uso de PII por anunciantes permite que eles indiquem os dados pessoais dos usuários que querem impactar com determinada propaganda. A perfilização deixa de ser por segmentos de usuários e passa a ser individualizada, sabendo os anunciantes quem receberá determinado conteúdo. O conceito de PII também pode ser ressignificado com o avanço das tecnologias de cruzamento de informações e inferência de dados. Tradicionalmente, PII era definido de forma estanque e imutável, atualmente existe o risco de que informações consideradas não PII possam ser transformadas em PII em um momento posterior, o que também aproxima a incidência das leis de proteção de dados⁵⁹.

Um caso emblemático sobre os efeitos dessas decisões automatizadas que definem o perfil do usuário e os anúncios que serão expostos a eles evidenciou desafios dessa nova forma de publicidade na campanha presidencial dos EUA por Ted Cruz e Donald Trump, em 2016, e nas campanhas do *Brexit* no Reino Unido, no mesmo ano⁶⁰. Por meio de ferramentas de publicidade direcionada do Facebook, foi possível que a Cambridge Analytica, empresa

⁵⁸ CHOI, Jin-A; LIM, Kiho. Identifying machine learning techniques for classification of target advertising. **ICT Express**, v. 6, n. 3, 2020, p. 175-180, p. 176.

⁵⁹ ANDREOU, Athanasios et al. Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations. **NDSS 2018 - Network and Distributed System Security Symposium**, Feb 2018, San Diego, United States. pp.1-15, p. 1. SCHWARTZ, Paul; SOLOVE, Daniel; The PII Problem: Privacy and a new concept of personally identifiable information. **New York University Law Review**, v. 86, 2011, p. 1814.

⁶⁰ PRIVACIDADE HACKEADA. **Direção de Karim Amer e Jehane Noujaim**. Estados Unidos: Netflix, 2019. (110 min)

inglesa de consultoria de marketing político, combinasse análise preditiva e comportamental com base na coleta de dados pessoais de usuários do Facebook. A partir dessa análise, a empresa foi capaz de direcionar aos cidadãos específicos propagandas de candidatos específicos adaptadas aos interesses desses eleitores por meio da rede social. Neste caso, o *profiling* foi utilizado para direcionamento de propaganda política personalizada e consequente influência no processo eleitoral⁶¹.

Decisões automatizadas também geram recomendações sobre, dentre uma série de itens, quais produtos são de interesse de usuários individualmente considerados, em vista de seu histórico de preferências ou outros elementos. Para ilustrar, em meados dos anos 2000, o sistema de recomendações da Amazon ficou conhecido por alterar a forma com que as pessoas adquirem livros *on-line*. Com o sucesso de vendas de um livro chamado *Into Thin Air*, o sistema de recomendação observou padrões no comportamento de compra dos usuário que gostavam desse livro e passou a recomendar também o livro *Touching the Void*, lançado a mais de 10 anos antes e que não havia chamado tanto a atenção dos consumidores à época. Porém, com o sistema de recomendação desenvolvido de forma automatizada e com base no comportamento dos consumidores e nas características do produto, foi criado um novo modelo econômico de recomendação de produtos para as indústrias de mídia e entretenimento, que antes apenas se restringia a promover conteúdos já conhecidos e populares em uma sociedade de massa⁶².

Sistemas de recomendação podem funcionar como verdadeiros filtros automatizados sobre o que consumir, assistir, escutar e opinar. Sobre esse fenômeno, Joseph Turow argumenta que o aumento da personalização de propagandas com base em perfis de consumidores opacos representa um risco para a sociedade e o discurso democrático, já que, ao “classificar” indivíduos em categorias pré-determinadas, a decisão automatizada de definição de perfis compartimentaliza a sociedade em grupos estanques⁶³. No entanto, ainda não está definido se sistemas automatizados de recomendação vinculados ao setor do entretenimento, como recomendação de vídeos, filmes, músicas, livros, podcasts e outros, serão percebidos enquanto decisões com relevância significativa à esfera de interesses dos

⁶¹ BOLDYREVA, Elena; GRISHINA, Natalia; DUISEMBINA, Yekaterina. Cambridge Analytica: ethics and online manipulation with decision-making process. **The European Proceedings of Social & Behavioural Sciences**, p. 91-102, dez., 2018, p. 95. Para mais informações, acesse: ALMEIDA, Eduarda. O caso Facebook e Cambridge Analytica e o direito à proteção de dados do consumidor. **Congresso de Iniciação Científica da Unb e Congresso de Iniciação Científica do DF**, Brasil, jan. 2022. Disponível em: <https://conferencias.unb.br/index.php/iniciacaocientifica/27CICUnB18df/paper/view/38766>.

⁶² ANDERSON, Chris. **The Long Tail**. 2004. Disponível em: <https://www.wired.com/2004/10/tail/>. Acesso em: 28 dez. 2022.

⁶³ TUROW, Joseph. **The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth**. Yale University Press, 2011.

titulares. Essa classificação teria como efeito a necessidade de observar as obrigações das leis de proteção de dados nesse sentido.

Porém, as condições evidenciadas pelo Grupo de Trabalho do Art. 29 para direcionamento de anúncios enunciadas no subtópico anterior podem ser aplicáveis: (i) a intrusividade do processo de elaboração do perfil; (ii) as expectativas e desejos das pessoas envolvidas; (iii) a forma como o anúncio é entregue, ou (iv) as vulnerabilidades particulares das pessoas visadas⁶⁴. Dessa forma, a depender desses critérios, um sistema que recomenda conteúdos para consumo de forma automatizada pode estar sujeito às obrigações de proteção de dados.

No setor de saúde, o projeto do Centro de Telessaúde do Hospital das Clínicas da Universidade Federal de Minas Gerais, que faz parte da Rede da Empresa Brasileira de Serviços Hospitalares vinculado ao Ministério da Educação, desenvolveu ferramenta de chatbot. Essa ferramenta, chamada de Telecovid-19, visa informar os usuários sobre a propagação da pandemia e avaliar o estado de saúde desses usuários por meio de um atendimento inicial que classificaria o estado do paciente por nível de prioridade como de emergência, urgência, casos moderados ou leves. Assim, por meio do aplicativo, o usuário informaria seu nome, idade e sexo e outras informações de saúde para que o sistema indicasse aqueles que deveriam procurar assistência médica e os que não. Isso “desafogaria” os serviços de urgência e evitar que pessoas aglomerassem em hospitais aumentando a chance de contaminação com a doença⁶⁵.

No Uruguai, foi desenvolvido o aplicativo Coronavirus UY como ferramenta para evitar a disseminação do Covid-19 a partir de funcionalidades mais complexas que o exemplo brasileiro, como: (i) a visualização de informações sobre o estado da pandemia no Uruguai; (ii) o relato de sintomas; (iii) a consulta por telemedicina e (iv) o alerta de exposição ao vírus se a pessoa encontrou com alguém infectado a pouco tempo⁶⁶. Este alerta é produzido a partir de tratamento automatizado de dados em que um usuário do aplicativo, quando infectado pela

⁶⁴ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 22. Disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963. Acesso em: 14 dez. 2021.

⁶⁵ BRASIL. Empresa Brasileira de Serviços Hospitalares. **Robôs virtuais de hospitais da Rede Ebserh/MEC fizeram quase nove mil atendimentos que auxiliam no combate à Covid-19**. 2021. Disponível em: <https://www.gov.br/ebserh/pt-br/comunicacao/noticias/robos-virtuais-de-hospitais-da-rede-ebserh-mec-fizeram-quase-nove-mil-atendimentos-que-auxiliam-no-combate-a-covid-19>. Acesso em: 27 dez. 2022.

⁶⁶ URUGUAI. Ministério de Salud Publica. **Información sobre la Aplicación Coronavirus UY**. 2020. Disponível em: <https://www.gub.uy/ministerio-salud-publica/politicas-y-gestion/informacion-sobre-aplicacion-coronavirus>. Acesso em: 10 jan. 2023.

doença, informava seu estado de saúde e, a partir disso, o sistema gerava alertas para celulares de pessoas que tiveram contato significativo com o infectado nos últimos 15 dias. Essa comunicação do infectado é voluntária e feita com o servidor do Coronavírus UY, que recebe os códigos que o celular emitiu nos últimos dias sem relacioná-los a nenhuma informação sobre os dispositivos ou pessoas que os utilizam. Dessa forma, o ministério da saúde do Uruguai destacou que não é uma pessoa que manda os alertas de risco de infecção, tendo acesso a essas informações, mas é o próprio celular que determina a necessidade de emitir⁶⁷, portanto é possível configurar esse tratamento como uma decisão automatizada.

Caso similar aconteceu na Finlândia. Uma empresa que provê serviços de saúde desenvolveu um sistema de processamento de dados dos pacientes para prevenção de doenças, e, diante do risco envolvido, essa empresa solicitou que a autoridade de proteção de dados avaliasse a conformidade do sistema com as normas de proteção de dados. Os pacientes em risco para sua saúde seriam identificados e encaminhados para tratamento através de um primeiro contato com o sistema. Os pacientes e seus registros médicos seriam analisados de forma automatizada a fim de identificar daqueles que estavam em situação de risco e assim definir uma lista de prioridades a fim de prevenir o aparecimento e a progressão de doenças e melhorar a equidade no sistema de saúde.

Para analisar se esse sistema implicava em decisões automatizadas, a autoridade finlandesa distinguiu dois cenários: casos em que (i) os pacientes seriam selecionados para exame posterior com base em uma avaliação de risco automatizada; e (ii) pacientes que não seriam selecionados após a avaliação de risco. Para o primeiro grupo, o resultado da análise seria levado em conta apenas como um elemento do processo de tomada de decisão, já que a decisão final seria tomada por uma pessoa treinada. Portanto, haveria intervenção humana relevante. Entretanto, o segundo grupo não estaria sujeito a uma avaliação por pessoa competente, logo estaria exposto a uma decisão automatizada baseada em dados pessoais. Ainda, a autoridade entendeu que a não admissão ao tratamento médico poderia ter efeitos adversos significativos sobre a saúde dos indivíduos e, por isso, ela produziria efeitos legais ou de similar importância para os pacientes que fossem rejeitados⁶⁸.

⁶⁷ URUGUAI. Ministério de Salud Publica. **Guía para usuarios de la aplicación Coronavirus UY**. 2020. Disponível em:

https://www.gub.uy/ministerio-salud-publica/sites/ministerio-salud-publica/files/2020-06/disen%CC%83o%20ga%20cetilla%20coronavirus%20%20copia_0.pdf. Acesso em: 10 jan. 2023.

⁶⁸ FINLÂNDIA. Tietosuojavaltuutetun toimisto. **3895/83/22**. Julgado em: 23.06.2022. Disponível em: https://gdprhub.eu/index.php?title=Tietosuojavaltuutetun_toimisto_%28Finland%29_-_3895%2F83%2F22. Acesso em: 27 dez. 2022. Decisão similar foi proferida pela autoridade finlandesa no caso 6482/186/2020.

Além disso, sistemas de IA estão sendo aplicados para auxiliar no diagnóstico de doenças, no entanto a tecnologia ainda está servindo como apoio à decisão humana, por isso não se encaixam na definição de decisões automatizadas. Devido aos avanços no poder computacional, nos algoritmos de aprendizagem e na disponibilidade de grandes conjuntos de dados (*big data*) derivados de registros médicos e monitores de saúde, é possível que a tecnologia auxilie profissionais da área de definição de diagnósticos e tratamentos de saúde. A implementação de ferramentas de IA na saúde já auxilia a detecção de doenças, classificação de doenças, processos de tomada de decisão na escolha de opções de tratamento⁶⁹, de forma a ser possível vislumbrar um cenário futuro em que será delegado à máquina essas atividades, mesmo sem supervisão humana.

Sistemas que se ocupam de tomar decisões de forma automatizada também estão sendo utilizados pela Administração Pública na gestão de políticas públicas. Um exemplo é o caso do Instituto Nacional do Seguro Social (INSS) que, em 2022, passou a utilizar ferramentas automatizadas para analisar dados pessoais dos cidadãos e, com isso, conceder ou não benefícios sociais, como aposentadorias, pensões e auxílios-doença. Com o uso da tecnologia, a fila de pedidos de aposentadoria em análise pelo INSS diminuiu 25%, porém a fila de recursos por indeferimento do pedido de aposentadoria cresceu 32%⁷⁰. Isso indica para a possibilidade de tomada de decisão automatizada inadequada e ineficiente, de forma que a pessoa que teve o benefício indeferido sairia da fila de pedidos de aposentadoria para a fila de revisão.

Na Dinamarca, um sistema algorítmico também está sendo utilizado pela *Udbetaling Danmark*, órgão responsável pela distribuição de benefícios sociais, para concessão ou recusa de benefícios de pensão e outros. Este caso foi analisado pela autoridade de proteção de dados do país, Datatilsynet, que entendeu pela violação do RGPD por falta de informação ao titular sobre a existência de decisões automatizadas⁷¹. Como evidenciado anteriormente, ferramentas automatizadas também foram utilizadas para pagamento do Auxílio Emergencial enquanto benefício social durante a pandemia do COVID-19. No entanto, esse exemplo chama atenção por não ter sido possível uma revisão da decisão tomada pelo sistema, apenas reanálise, já que

⁶⁹ KUMAS, Yogesh *et al.* Artificial intelligence in disease diagnosis: a systematic literature review, synthesizing framework and future research agenda. **Journal of Ambient Intelligence and Humanized Computing**, Springer, 2022, p. 21.

⁷⁰ LUDER, Amanda. **Robô que analisa processos do INSS causa aumento de recursos por indeferimento**. 2022. Disponível em: <https://g1.globo.com/economia/noticia/2022/10/07/robo-que-analisa-processos-do-inss-causa-aumento-de-recursos-por-indeferimento.ghtml>. Acesso em: 27 dez. 2022.

⁷¹ DINAMARCA. Datatilsynet. **2019-421-0028**. Publicado em: 26.02.2020. Disponível em: https://gdprhub.eu/index.php?title=Datatilsynet_-_2019-421-0028. Acesso em: 28 dez. 2022.

o sistema não permitia que o titular complementasse ou alterasse alguma informação, apenas que submetesse novo pedido com base nos mesmos dados inseridos adicionalmente⁷².

Além disso, decisões automatizadas também são utilizadas no âmbito da educação para, por exemplo, verificar a presença dos estudantes em escolas municipais por meio da tecnologia de reconhecimento facial automatizada, que registra a presença dos estudantes a partir da leitura digital das informações faciais de forma automática e sem interferência humana. Esse sistema de aferição de presença foi utilizado pelo município de Pilar, em Alagoas, Recife, no Pernambuco, Anápolis, no Goiás, e em escolas estaduais espalhadas pelo Tocantins⁷³.

Em Londres, algoritmos foram utilizados para projetar notas dos estudantes em testes que determinavam acesso às universidades do Reino Unido, diante do contexto de pandemia que impossibilitou a realização das provas finais de forma presencial. O sistema utilizou informações como o histórico de desempenho geral de um determinado centro de ensino combinado com o desempenho de estudantes individuais, entre outras informações, para um modelo estatístico que previu as notas dos estudantes. No entanto, o uso do sistema foi seguido de protesto pelos estudantes, que questionaram os parâmetros utilizados pelo algoritmo, que se valeu, por exemplo, de dados de antigos alunos da mesma escola para a atribuição de notas individuais⁷⁴. Esse é um caso interessante para perceber-se como as decisões automatizadas estão sendo utilizadas para definir acesso a oportunidades de pessoas no presente com informações de pessoas do passado.

Um caso de uso de decisão automatizada no âmbito escolar foi levado a análise da autoridade de proteção de dados de Portugal. A escola em questão utilizou ferramentas de uma empresa norte-americana, Respondus, para verificar o ambiente de prova durante as avaliações *on-line* realizadas pelos estudantes durante a pandemia. O sistema monitorava os movimentos do estudante e seus arredores, obtinha informações do dispositivo (atividade do teclado, atividade do mouse, modificações de *hardware*) para identificar padrões, analisava a interação dos estudantes com o exame, incluindo contagem de tempo e mudança de respostas, bem como comparava as respostas entre os estudantes. Todos esses dados eram tratados de

⁷² TAVARES, Clarice *et al.* **O Auxílio Emergencial no Brasil: Desafios na implementação de uma política de proteção social datificada**. 2022.p. 21. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/01_Informe-Brasil_Inteligencia-Artificial-e-Inclusao_PT_22042022.pdf. Acesso em: 15 dez. 2022

⁷³ REIS, Carolina *et al.* **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil**. Brasília: Laboratório de Políticas Públicas e Internet, 2021, p. 56 - 59.

⁷⁴ SIMONITE, Tom. **Skewed Grading Algorithms Fuel Backlash Beyond the Classroom**. 2020. Disponível em: <https://www.wired.com/story/skewed-grading-algorithms-fuel-backlash-beyond-classroom/>. Acesso em: 28 dez. 2022.

forma automatizada a fim de se gerar um relatório da sessão de avaliação de cada estudante que indicava um *score* sobre a sessão de prova para auxiliar o professor a determinar o risco de desvios durante a execução da prova. Essa decisão de *score* do sistema foi percebida como decisão automatizada pela autoridade, já que, segundo ela, a “falta de critérios norteadores para os docentes tomarem decisões coerentes e transparentes pode ser geradora de discriminação e permitir que o docente por regra valide a decisão automatizada do sistema”, sem questionar o resultado do relatório, de forma a tornar a interferência humana não suficientemente válida⁷⁵.

As decisões automatizadas estão sendo utilizadas em diversos âmbitos na vida cotidiana. Nesta seção, foram destacados os seguintes setores: bancário, de seguro, de crédito, aplicativos de transporte e entrega, publicidade, entretenimento, saúde, políticas públicas, e de educação. Essa lista não é exaustiva e não busca apresentar usos com maior impacto nos direitos dos cidadãos, já que, apesar de largamente utilizados, não serão objetos de análise nesta pesquisa os usos de decisões automatizadas no âmbito penal e criminal, seja para segurança pública ou persecução penal.

Nesse sentido, a classificação de uma decisão automatizada como sendo regulada ou não pelas normas de proteção de dados, inclusive a LGPD, ocorre de maneira específica quando observado o caso concreto. Não é possível perceber abstratamente quando as decisões são tomadas por máquinas sem intervenção humana relevante e que se utilizam de dados pessoais. Além disso, não há consenso sobre quando se está diante de uma decisão que impacta relevantemente os interesses dos titulares, sendo necessária uma análise caso a caso para avaliar os impactos da escolha de um sistema automatizado para a vida de uma pessoa. O mesmo conjunto de dados pode dar origem a uma decisão considerada relevante em um contexto diante de seu resultado, mas em outro cenário não. A título de exemplo, como explicitado anteriormente, o Tribunal Distrital de Amsterdã julgou não se tratar de decisão automatizada relevante sistema de pareamento de usuários motoristas e passageiros de aplicativo de transporte de pessoas, mas a autoridade italiana entendeu ser relevante a decisão automatizada que prioriza o acesso de certos usuários entregadores na seleção de quem irá entregar produtos em horário de pico por interferir nos seus interesses econômicos.

⁷⁵ UNIÃO EUROPEIA. Comissão Nacional de Proteção de Dados. **Deliberação/2021/622**. Julgado em: 11.05.2021. Disponível em: <https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887>. Acesso em: 28 dez. 2022.

2.4. Os influxos da LGPD nas decisões automatizadas

Entre esses e outros casos concretos não evidenciados no subtópico anterior (tópico 2.3), fica evidente que decisões automatizadas são ferramentas utilizadas em diferentes contextos para a escolha consistente de um resultado, *output*. Para tanto, regras são determinadas e traduzidas em algoritmos, que funcionam com base em um volume expressivo de dados pessoais e com capacidade de aprendizado para atender um objetivo específico programado. Esses sistemas funcionam para medir ou avaliar comportamentos, ações, ou informações de pessoas para, a partir desse *score*, definir recomendações aos titulares, prioridade de ações às empresas ou a forma de acesso a produtos e serviços de forma personalizada. A capacidade da IA de levar em consideração grande quantidade de dados e combiná-los para determinada finalidade é superior a dos humanos⁷⁶, podendo tornar a tomada de decisão mais rápida e precisa. Associado às funcionalidades e aos benefícios, ficou evidente que essas decisões também apresentam riscos para os titulares submetidos a elas, inclusive na esfera jurídica de direito de proteção de dados e no fundamento da autodeterminação informativa, objetos da LGPD.

Um dos objetivos da lei brasileira é justamente estabelecer ferramentas jurídicas para conter os efeitos negativos que decisões automatizadas podem implicar aos interessados. Nesse sentido, a lei estabelece uma série de princípios (art. 6º) que orientam todo o ciclo de vida dos dados pessoais, sensíveis ou não, tratados pelos controladores, responsáveis por decidir sobre o processamento das informações (art. 5º, VI), seja o compartilhamento (art. 5º, XVI), transferência internacional (art. 33 a 36), ou descarte desses dados (art. 15). Além disso, a lei define as hipóteses legais que autorizam o tratamento (art. 7º e 11), os direitos dos titulares (art. 9º, 17 a 22) e as ferramentas disponíveis para garantir a devida proteção de dados, como o registro das atividades de tratamento (art. 37), o relatório de impacto à proteção de dados (art. 38), as medidas de segurança (art. 46 a 49) e documentos que promovem as boas práticas e a governança (art. 50 e 51), observando as peculiaridades dos titulares quando crianças e adolescentes (art. 14) e quando controladores membros da Administração Pública (art. 23 a 30).

Todo esse arcabouço regulatório incide sobre decisões tomadas de forma automatizada com base em dados pessoais, de forma a ser necessário adaptar essas práticas às normas da LGPD, sob pena de estar em desconformidade com ela. Dentre os principais riscos à proteção

⁷⁶ PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária accountability. **Revista de Informação Legislativa**, v. 57, n. 225, p. 43-60, jan./mar. 2020, p. 58. Disponível em: https://www12.senado.leg.br/ril/edicoes/57/225/ril_v57_n225_p43.pdf. Acesso em: 29 dez. 2022.

de dados, destacam-se (i) a vigilância; (ii) a discriminação e (iii) a opacidade desses sistemas de decisão. Esses riscos estão associados à desafios éticos no uso de IA⁷⁷, porém também estão ligados aos fundamentos de regulação da proteção de dados, na medida em que são consequência do tratamento indevido de informação pessoal. Sistemas que promovem esses riscos não observam os limites impostos pelos princípios da LGPD, que serão analisados de forma mais detida nos próximos tópicos, como o da finalidade, necessidade e adequação, não discriminação, transparência e prestação de contas.

A vigilância ocorre com a coleta de volume expressivo de dados não associados ou desproporcionais a uma finalidade específica, de forma que o tratamento dessas informações pessoais resulte em produto rentável de predição de comportamento humano⁷⁸ e, com isso, falta de autonomia do próprio titular sobre suas escolhas⁷⁹. Esse estado está associado ao cenário de capitalismo de vigilância percebido por Shoshana Zuboff, em que é instaurado um novo modelo de mercado que reconfigura as relações de poder existentes ao conhecer detalhes da personalidade e comportamento humano para, assim, determinar a forma de ser das pessoas. Yuval Harari percebe que o senso de autonomia e vontade estão em transformação em um contexto de *big data*. Para ele, há uma transição do motor responsável pela tomada de decisão humana, e agora estaria na vontade de algoritmo, período chamado de “dataísmo”. Nesse novo cenário, acredita-se que, por meio de dados biométricos e poder computacional suficiente, o sistema algoritmo abrangente poderia entender os humanos muito melhor do que eles próprios e, assim, determinar as ações humanas⁸⁰.

Os limites impostos pelos princípios da finalidade, necessidade e adequação, analisados adiante neste pesquisa (tópico 4.1.2), não são observados em cenários de vigilantismo, já que o tratamento de dados excede o necessário para se atingir um objetivo

⁷⁷ Os seguintes artigos se ocupam dos desafios éticos impostos pela IA: FLORIDI, Luciano *et al.* AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. **Minds and Machines**, n. 28, 2018. MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. **Suprema: revista de estudos constitucionais**, v. 1, n. 1, p. 154-180, jan./jun. 2021. Disponível em: <https://suprema.stf.jus.br/index.php/suprema/article/view/20/18>. Acesso em: 29 dez. 2022. HERIK, Jaap van den; LAAT, Cees de. The future of ethical decisions made by computers. In: JANSSENS, Liisa (ed.). **The Art of Ethics in the Information Society**. Amsterdam: Amsterdam University Press, 2016. BIETTI, Elettra. From Ethics Washing to Ethics Bashing: A Moral Philosophy View on Tech Ethics. **Journal of Social Computing**, v. 2, n. 3, pp. 266-283, 2021. DONEDA, Danilo *et al.* Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018. RICHARDS, Neil M.; KING, Jonathan. Big Data Ethics. **Wake Forest Law Review**, v. 49, n. 393, 2014.

⁷⁸ ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. Estados Unidos: Perseus Books, LLC, 2021, chapter 13, instrumentalism as a new species of power.

⁷⁹ Para mais informações, acesse: HARARI, Yuval. **Yuval Noah Harari on big data, Google and the end of free will**. 2016. Disponível em: <https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c>. Acesso em: 29 dez. 2022.

⁸⁰ ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. Estados Unidos: Perseus Books, LLC, 2021. chapter 18, freedom and knowledge.

expresso e diversos dados, de diversas fontes, passam a ser utilizados para supervisionar o titular. Para evitar esse cenário, mas ao mesmo tempo atender a forma de funcionamento das ferramentas de aprendizado de máquinas, é importante adotar um modelo que avalie criticamente a natureza e a quantidade de dados utilizados, reduzindo dados redundantes ou marginais e apenas aumentando gradualmente o tamanho do conjunto de dados de treinamento⁸¹.

Outra questão evidenciada pelo uso de decisões automatizadas é a possibilidade de efeitos discriminatórios no uso da ferramenta, ou seja, a tendência de algoritmos produzirem resultados que levam a uma desvantagem para grupos sociais específicos, tais como mulheres, pessoas com pele escura, minorias étnicas ou pessoas com deficiência⁸². O uso de algoritmos na tomada de decisão, por mais que se espere maior objetividade e neutralidade no resultado, pode indicar soluções com viés prejudicial para um grupo. Com isso, os sistemas não funcionariam de forma adequada quando aplicados em casos concretos, causando discriminação ilícita ou abusiva e violação de direitos. O desenvolvimento de viés, especialmente em sistemas de aprendizado de máquinas, pode estar associado (i) aos dados pessoais utilizados para treinar e verificar a acurácia do sistema não serem representativos ou refletirem discriminações preexistentes; (ii) à seleção inadequada dos atributos a serem considerados pelo algoritmo ou (iii) à definição do objetivo que se deseja alcançar com a decisão automatizada⁸³. Essa forma de tratamento de dados viola diretamente o princípio da não-discriminação, especificado de forma mais detida no quarto tópico (tópico 4.1.3) desta pesquisa.

Em regra, os sistemas algoritmos são opacos, ou seja, não há transparência ou maior visibilidade sobre como os resultados são alcançados e os fatores que influenciam a escolha final. Essa opacidade pode ser causada por, em regra, três características: (i) mecanismos de proteção patrimonial ou sigilo comercial sobre o algoritmo enquanto ferramenta de solução de problemas; (ii) capacidade de entendimento sobre o código do algoritmo em sua forma matemática; (iii) descompasso entre procedimentos matemáticos e técnicos de algoritmos de

⁸¹ UNIÃO EUROPEIA. Conselho da Europa. **Artificial Intelligence and data protection**. 2019. Disponível em: <https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7>. Acesso em: 29 dez. 2022, p. 24

⁸² UNIÃO EUROPEIA. European Union Agency for Fundamental Rights. **Bias in Algorithms – Artificial Intelligence and Discrimination**. Luxembourg: Publications Office of the European Union, 2022, p. 17

⁸³ HAO, Karen. This is how AI bias really happens – and why it’s so hard to fix. **MIT Technology Review**, 2014. Disponível em: <https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/>. Acesso em: 30 dez. 2022.

aprendizagem de máquinas e a forma de interpretação semântica humana⁸⁴. Em atenção a esse risco, a LGPD estabelece deveres de transparência e informação (tópico 4.1.1) para evitar que o titular não conheça minimamente o tratamento de dados que está submetido.

Essa opacidade, bem como os outros dois riscos pontuados nesta seção, pode colocar em cheque a confiança dos titulares e da sociedade nos sistemas algoritmos, já que não se sabe e não se controla o impacto e as próprias decisões automatizadas no comportamento humano. Ter evidências sobre a forma de decisão é especialmente caro ao âmbito jurídico, uma vez que a validade das decisões se baseia no processo que levou àquela escolha e na fundamentação específica dessa escolha⁸⁵.

Esses riscos, em especial a opacidade, que se relaciona diretamente com o objetivo desta pesquisa, desafiam os direitos fundamentais de liberdade e autonomia, privacidade e proteção de dados dos titulares, de forma que estes passariam a não mais ocupar posição de protagonismo na decisão sobre quem, como, e quais dados seriam tratados por terceiros. Esses questionamentos guardam origem nas próprias discussões sobre o desenvolvimento da matéria de proteção de dados e a autodeterminação informativa, enquanto consectário do direito de personalidade e garantidor da possibilidade do titular se autodeterminar frente ao tratamento automatizado de dados pessoais. Essa atividade, desde meados dos anos 60 e 70, chamou atenção dos juristas à época diante dos desafios que ela impunha à capacidade do titular autodeterminar-se.

A autodeterminação não é uma noção circunscrita a um tipo de tratamento de dados específico e datado, de forma a assumir novos contornos quando aplicada à cenários de decisões automatizadas, sistemas de IA e *big data*, em que a coleta do consentimento não é suficiente. Ao mesmo tempo em que há flexibilidade no conceito, a autodeterminação pode ser reduzida de forma expressiva com o uso massivo e sem salvaguardas de decisões automatizadas, as quais deixam de apenas prever o futuro para determinar o presente e, com isso, alteram comportamentos humanos para acomodar as rotinas facilitadas pelos algoritmos⁸⁶. Diante disso, a capacidade dos titulares para agirem autonomamente pode se ver minada pelas novas formas de controle exercidas por aqueles que detém dados pessoais em larga escala.

⁸⁴ BURRELL, Jenna. How the machine ‘thinks’: Understanding opacity in machine learning algorithms. **Big data and Society**, jan.-jun., 2016, p. 3.

⁸⁵ FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. **Suprema: revista de estudos constitucionais**, v. 1, n. 1, p. 154-180, jan./jun. 2021. Disponível em: <https://suprema.stf.jus.br/index.php/suprema/article/view/20/18>. Acesso em: 29 dez. 2022, p. 171

⁸⁶ DONEDA, Danilo *et al.* Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018, p. 11.

3. O SENTIDO ATRIBUÍDO À AUTODETERMINAÇÃO INFORMATIVA NA PROTEÇÃO DE DADOS

A autodeterminação informativa é um dos fundamentos da disciplina de proteção de dados positivado no art. 2º, II, da LGPD. Esse conceito é um dos pilares da matéria de proteção de dados e tem como objetivo justamente “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, conforme o art. 1º, da lei. Dessa forma, esta pesquisa analisa, por meio das lentes da autodeterminação informativa, garantida pela LGPD e pela Constituição Federal, os desdobramentos e as delimitações desse conceito quando aplicado ao direito à explicação.

A partir desse conceito e da interpretação dada a ele desde sua concepção, é possível delimitar as suas implicações na formulação de uma lei geral que visa regular o devido tratamento de dados pessoais no Brasil. Os princípios e os direitos de proteção de dados, enquanto mecanismos primordiais para garantia da conformidade com a lei, são consequências diretas da aplicação da autodeterminação sobre as informações do titular, por isso serão objeto de estudo desta pesquisa (tópico 4).

3.1. A origem do conceito da autodeterminação informativa

A consolidação da autodeterminação informativa enquanto direito dos indivíduos é resultado de fluxos e influxos direcionados a solução de casos concretos em que os mecanismos de garantia de um direito de privacidade como liberdade negativa não eram suficientes para os desafios enfrentados pela sociedade. Esses casos estavam sendo debatidos principalmente em países em que havia disseminação de instrumentos informáticos que, inicialmente, estavam disponíveis para o setor público, mas que logo passaram a ser utilizados por entidades e empresas privadas.

A capacidade de processamento de dados foi um dos impulsionadores do tema de proteção de dados, uma vez que, com a disseminação dos dispositivos eletrônicos, os riscos associados ao processamento automatizado e em massa de dados se intensificaram, assim como o número de pessoas afetadas. Inicialmente, essas ferramentas eram acessíveis a órgãos estatais, mas logo o poder de processamento de dados ganhou relevância nas empresas privadas. O formato das regulações de proteção de dados é um espelho desse movimento. Nesse sentido, a Professora Laura Schertel indica que, apesar das primeiras leis de proteção de dados se justificarem pelo “temor do poder de processamento de dados pelo Estado, logo

se viu que o perigo também residia no setor privado”⁸⁷. Tendo isso em vista, esta pesquisa analisa o surgimento do tema nos Estados Unidos da América (EUA), que registra debates sobre os limites de intrusão na vida privada na década de 1960, e na Alemanha, país responsável pela popularização do conceito a partir de 1983.

Em 1967, o Professor Alan Westin definiu privacidade como a pretensão de indivíduos, grupos ou instituições em determinarem por si mesmos quando, como e até que ponto as informações sobre eles são comunicadas a terceiros enquanto ser social, que compartilha informações pessoais na sociedade em que vive⁸⁸. Esse conceito é diferente das noções tradicionais de privacidade associadas ao direito de ser deixado só, defendido por Warren e Brandeis, ainda em 1890. Nesta definição, a privacidade seria um direito de liberdade negativa do indivíduo de não ser incomodado por terceiros a respeito de ações praticadas no âmbito íntimo⁸⁹. Houve uma mudança de perspectiva sobre o objeto do direito de privacidade, que antes estava ligada à informação privada enquanto não passível de ser conhecida pelo público, e passa a estar relacionada à possibilidade do titular escolher e controlar a informação pessoal conhecida por terceiros.

Em observância a essa noção de participação do titular, o relatório *Records, Computers and the Rights of Citizens* do Departamento de Saúde, Educação e Bem-estar dos EUA, em 1973, buscou conciliar essa faceta da privacidade com a gestão de políticas públicas na área da saúde diante do uso de computadores para manter registros sobre os cidadãos. O relatório identifica que necessariamente dados pessoais seriam divulgados pelos seus titulares e que caberia a eles decidir a natureza e a extensão de tal divulgação. A privacidade não é contrária à divulgação e, portanto, ao uso de dados pessoais. Dessa forma, deveria ser previsto um mecanismo em que o indivíduo possa descobrir quais informações sobre ele estão em um registro e como elas são utilizadas. Ainda, seria possível que o titular impedisse o uso de suas informações obtidas para um propósito mas disponibilizadas para outros fins sem seu consentimento. As conclusões deste relatório serviram de base para a identificação dos *Fair Information Principles*, os quais foram a base para formulação de consensos iniciais sobre o devido tratamento de dados em acordo com um quadro mínimo de proteção de dados pessoais

⁸⁷ MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado) - Faculdade de Direito da Universidade de Brasília, 2008, p. 133-134. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso: 10 nov. 2022.

⁸⁸ WESTIN, Alan. **Privacy and freedom**. New York: Ig Publishing, 1967, p. 24. Disponível em: <https://dokumen.pub/privacy-and-freedom-1632460734-9781632460738.html>. Acesso em: 11 nov. 2022.

⁸⁹ WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, vol. , n. 5, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 10 nov. 2022.

a nível internacional⁹⁰. As ideias de procedimentos de controle são similares aos efeitos do caso alemão, que reconheceu um direito da pessoa se autodeterminar por meio de suas informações pessoais conhecidas por outras pessoas, como será analisado a seguir.

Em 1983, o Tribunal Constitucional Federal alemão proferiu sentença no caso Recenseamento em que passou a reconhecer expressamente o direito à autodeterminação informativa. Esse direito foi percebido a partir de uma interpretação do art. 2º, §1º, combinado com o art. 1º, §1º, da Lei Fundamental da República da Alemanha. O primeiro dispositivo, relativo aos direitos de liberdade, garante a todos o “direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral”⁹¹. Já o §1º, do art. 1º, prevê que “a dignidade da pessoa humana é intangível. Respeitá-la e protegê-la é obrigação de todo o poder público”⁹². Esses dispositivos fundamentaram uma decisão que é um dos marcos para o desenvolvimento da matéria de proteção de dados pessoais e um expoente do direito à autodeterminação informativa no Brasil, por isso será analisada de forma detida nesta pesquisa.

O objeto enfrentado pela corte no caso em questão era a Lei do Censo, de 25 de março de 1982, o qual dispunha sobre o recenseamento geral da população, das profissões, das residências e dos locais de trabalho para fins estatísticos. Essa lei objetivava a identificação de dados demográficos da Alemanha, como dados relacionados à distribuição da população no território e as atividades econômicas realizadas pelos cidadãos. A finalidade da coleta dos dados era a elaboração de políticas públicas e de decisões político-econômicas em acordo com as necessidades específicas da população.

Para tanto, pesquisadores credenciados coletariam dados da população, como endereço, estado civil, filiação à religião, nacionalidade, fonte de subsistência, além de dados profissionais, como local de trabalho, tempo gasto para ir ao trabalho, meio de transporte usado e horário de trabalho. Todos os adultos ou menores que vivessem em casa própria estariam obrigados a fornecer essas e outras informações. As pessoas empregadas no processamento de dados estariam proibidas de processar dados pessoais sem autorização para um propósito diferente da finalidade do respectivo desempenho de tarefa legal. Ainda, os

⁹⁰ ESTADOS UNIDOS DA AMÉRICA. **Records, Computers and the Rights of Citizens**. Department of Health, Education and Welfare, 1973, p. 40. Disponível em:

<https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 10 nov. 2022.

⁹¹ ALEMANHA. **Lei Fundamental da República da Alemanha**. 1949. Disponível em: <https://www.btg-bestellservice.de/pdf/80208000.pdf>. Acesso: 11 nov. 2022.

⁹² ALEMANHA. **Lei Fundamental da República da Alemanha**. 1949. Disponível em: <https://www.btg-bestellservice.de/pdf/80208000.pdf>. Acesso: 11 nov. 2022.

dados poderiam ser confrontados com registros públicos e poderiam ser transmitidos, quando anônimos, a repartições públicas para determinadas finalidades de execução administrativa⁹³.

No entanto, logo que a lei do censo foi promulgada, foram propostas diversas reclamações constitucionais no tribunal constitucional que defendiam a inconstitucionalidade da lei por violar direitos fundamentais dos reclamantes. O objeto das reclamações era, especialmente, o direito ao livre desenvolvimento da personalidade, previsto no art. 2º, §1º, da Lei Fundamental⁹⁴. Para a corte, esse questionamento de constitucionalidade da lei pode estar associado a um desconhecimento generalizado sobre o escopo, os propósitos da pesquisa e a necessidade de informações confiáveis para formulação do planejamento público. Além disso, os especialistas entendiam que a lei censitária de 1983, apesar de aprovada por unanimidade pelas autoridades legislativas, não atendia suficientemente aos requisitos constitucionais em termos das disposições sobre a coleta e o uso de dados⁹⁵.

A corte entendeu pela constitucionalidade da lei, tendo em vista que, na interpretação dos magistrados, a legislação impugnada corresponderia aos requisitos de clareza jurídica e proporcionalidade e não conduziria à catalogação da personalidade incompatível com a dignidade da pessoa humana. Ao mesmo tempo, para garantir o direito à autodeterminação informativa, seriam necessárias precauções processuais adicionais na implementação e na organização da coleta de dados. Como disposto em lei, as regras de transmissão de dados violariam os direitos gerais da personalidade, porque não estaria claro na lei como ocorreria a transferência de dados para fins administrativos, nem quais os propósitos claramente definidos para esse compartilhamento⁹⁶.

Diante das condições do tratamento de dados à época, a corte entendeu que a proteção dos indivíduos contra a coleta, o armazenamento, o uso e a divulgação ilimitados de seus dados estaria coberta pelo direito geral de personalidade previstos no art. 2º, §1º, e no art. 1º, §1º, da Lei Fundamental. A Alemanha estava passando por processo de intensificação do processamento automatizado de dados em que os processos decisórios eram apoiados cada

⁹³ ALEMANHA. **Volkszählungsgesetz 1983**. 1983. Disponível em: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//%5B@attr_id=%27bgbl182s0369.pdf%27%5D#_bgbl_%2F%2F*%5B%40attr_id%3D%27bgbl182s0369.pdf%27%5D_1668075101860. Acesso em: 11 nov. 2022.

⁹⁴ As seguintes reclamações foram propostas: 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83. Todos os processos foram julgados de maneira conjunta na decisão analisada nesta pesquisa.

⁹⁵ ALEMANHA. Entscheidungen der amtlichen Sammlung 65, 1 (71), **Recenseamento**. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 11 nov. 2022.

⁹⁶ ALEMANHA. Entscheidungen der amtlichen Sammlung 65, 1 (71), **Recenseamento**. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 11 nov. 2022.

vez mais em dados eletrônicos. Estes poderiam ser consultados e armazenados com facilidade, além de poderem ser combinados e integrados com outros. Isso permitiria a construção de um “quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida pudesse controlar suficientemente sua exatidão e seu uso”⁹⁷. Nesse sentido, essa combinação de direitos previstos na Lei Fundamental garantiria o poder do indivíduo decidir por si mesmo sobre a divulgação e o uso de seus dados pessoais, que resultaria no direito à autodeterminação informativa. No entanto, as concretizações jurisprudenciais feitas pela corte até então não circunscreveram o conteúdo do direito da personalidade de forma taxativa direcionada para o poder do indivíduo, decorrente da idéia de autodeterminação, de decidir por si próprio, quando e dentro de que limites os fatos relacionados a si próprio seriam revelados.

A corte entendia dever ser possível que as pessoas determinassem com segurança as informações as quais terceiros conhecem delas em certas áreas de seu meio social. Entendia-se que a falta de ferramentas para as pessoas avaliarem o nível de conhecimento de possíveis parceiros na comunicação poderia inibir substancialmente a “sua liberdade de planejar ou decidir com autodeterminação”⁹⁸. Ao mesmo tempo, o tribunal entendeu que o Estado não estaria proibido de coletar dados pessoais e de regular a sua utilização, como na lei do censo. O legislador, ao editar as normas, pode compreender o censo como um pré-requisito para o funcionamento sistemático da ação governamental. A legislatura pode pesar o interesse do indivíduo em permanecer privado ou anônimo em relação ao interesse do público em geral pela informação e, com isso, decidir pela necessidade de um censo a fim de atender esse interesse de informação.

Em vista dessa escolha legislativa, o tribunal entendeu não poder confiar apenas no controle do tipo de informação coletada pelo Estado, a definição dos usos possíveis desses dados é decisiva para uma conformidade entre a atuação do Estado e um direito à autodeterminação. A forma de uso dos dados depende, por um lado, da finalidade a que se destina a pesquisa estatística e, por outro, das opções de processamento e vinculação inerentes à tecnologia da informação. O uso dos dados pessoais deve estar restrito à finalidade prevista na lei do censo, de forma a proteger o indivíduo “contra o afastamento do propósito inicial de

⁹⁷ MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005.p. 237. Disponível em: <https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50-anos-de-jurisprudencia-do-tribunal-constitucional-federal-alemao.pdf>. Acesso em: 11 nov 2022.

⁹⁸ MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005, p. 237. Disponível em: <https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50-anos-de-jurisprudencia-do-tribunal-constitucional-federal-alemao.pdf>. Acesso em: 11 nov 2022.

levantamento de dados, mediante proibição de transmissão e de utilização”, além do dever de informação e do direito de apagamento dos dados⁹⁹. Como resultado, um dado irrelevante em si mesmo pode adquirir um novo significado e, por isso, a corte conclui que não há mais nenhum dado o qual pudesse ser considerado irrelevante nas condições de processamento automático dessas informações.

O direito à autodeterminação informativa não é absoluto ou ilimitado. A corte indica que as restrições a esse direito seriam permitidas quando existente um interesse predominante da coletividade. Essas limitações exigem uma base legal constitucional a qual deve corresponder aos requisitos do Estado de Direito de clareza normativa e de proporcionalidade das normas. Cabe ao legislador tomar precauções organizacionais e processuais para neutralizar o risco de violação de direitos de personalidade. Quanto aos requisitos constitucionais para tais restrições, deve ser feita uma distinção entre os dados pessoais que são coletados e tratados de forma individualizada e não anônima e os dados os quais se destinam a fins estatísticos. Isso porque, ao contrário dos dados individualizados, no levantamento de dados para propósitos estatísticos, não se pode exigir uma vinculação a uma finalidade estrita de tratamento, já que não são determináveis no momento da coleta¹⁰⁰.

O Tribunal Constitucional Federal Alemão fixou, por meio deste julgamento, a autodeterminação informativa como direito geral de personalidade protegido constitucionalmente a partir dos princípios expressos da dignidade humana e do livre desenvolvimento da personalidade. Esse direito garante ao titular o poder de determinar o fluxo de suas informações pessoais na sociedade e, com isso, mitigar os riscos de armazenamento ilimitado de dados e de formação de um retrato da pessoa, mesmo sem sua participação ou conhecimento¹⁰¹.

A partir dessa decisão, Veridiana Alimonti identifica seis elementos relevantes para desenvolvimento da matéria de proteção de dados: (i) a formulação do direito à autodeterminação informativa se deu a partir do direito geral de personalidade conjugado com a autodeterminação e a tutela do dado pessoal de forma abrangente; (ii) o conhecimento do

⁹⁹ MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005, p. 240. Disponível em: <https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50-anos-de-jurisprudencia-do-tribunal-constitucional-federal-alemao.pdf>. Acesso em: 11 nov 2022.

¹⁰⁰ ALEMANHA. Entscheidungen der amtlichen Sammlung 65, 1 (71), **Recenseamento**. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 11 nov. 2022.

¹⁰¹ MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado) - Faculdade de Direito da Universidade de Brasília, 2008, p. 47. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso: 10 nov. 2022.

contexto de utilização dos dados é mais relevante do que o tipo dos dados para determinar o risco que o tratamento oferece à personalidade; (iii) a proteção dos dados abrange o poder de decisão consubstanciado no direito à autodeterminação informativa; (iv) a autodeterminação é um poder do indivíduo inserido em sua comunidade social; (v) há necessidade de precauções organizacionais e processuais; (vi) a confiança na relação entre titular e responsável pelo tratamento deve ser protegida¹⁰².

Esses elementos foram consolidados na doutrina e nas regulações sobre proteção de dados pessoais ao redor do mundo, de forma a estabelecerem os fundamentos e objetivos dos direitos relacionados à autodeterminação que surgiram a partir de então. Mayer-Schoneberger identificou, na evolução da matéria na Europa, três gerações de regulação sobre a proteção de dados pessoais. Na primeira, a regulação de proteção de dados se concentrou em regular a tecnologia, a qual, na época, era o computador. Este deveria ser regulado e controlado por alto poder de processamento de dados pessoais e isso colocar em risco interesses das pessoas. Já a segunda geração é focada no direito individual de privacidade dos cidadãos enquanto liberdade negativa, de forma a ser necessário proteger o espaço de intimidade do indivíduo. Na terceira e última, impulsionada pelo julgamento do caso do Recenseamento e pela ideia de autodeterminação informativa, busca-se proteger os direitos de participação do titular de dados nas fases do tratamento de dados.¹⁰³

Antes da decisão da corte, o conceito de autodeterminação informativa havia sido empregado em parecer de Steinmuller e outros autores ao Ministério do Interior da Alemanha, em 1971, a respeito da forma jurídica de uma futura lei de proteção de dados. No parecer, os autores reconhecem a existência de um direito de autodeterminação do cidadão em decidir sobre seus dados pessoais. Esse direito teria incidência, especificamente, sobre quais dados serão tratados, quem os trataria e sob quais circunstâncias. Esse direito estaria ameaçado na medida em que outra entidade passasse a manipular um volume expressivo de informações sobre o titular e, com isso, passasse a exercer influência sobre essa pessoa¹⁰⁴.

A nível jurisprudencial, a decisão da corte alemã foi resultado do reconhecimento de um direito ao respeito à esfera privada enquanto direito de personalidade, separado do direito

¹⁰² ALIMONTI, Veridiana. **Algoritmos e autodeterminação: uma contribuição a partir das noções de autodeterminação informativa e controle no contexto de decisões automatizadas**. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, 2022, p. 156

¹⁰³ MAYER-SCHONEBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip; ROTENBERG, Marc. (ed.). **Technology and Privacy**. The New Landscape. Cambridge: MIT Press, 1997.

¹⁰⁴ STEINMULLER *et al.* **Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern**. BTdrucks VI/326, anexo 1, 1972, p. 88. Disponível em: <https://dserv.bundestag.de/btd/06/038/0603826.pdf>. Acesso em: 11 nov. 2022.

de liberdade geral de ação. Essa diferenciação é relevante para o desenvolvimento de um direito de personalidade e das proteções decorrentes dele. A noção de um direito de liberdade de ação garante o livre comportamento do indivíduo, mas não o protege contra ações de terceiros. Enquanto isso, um direito de personalidade também é aplicável em face da intervenção de terceiros¹⁰⁵. Esse direito à esfera privada também foi reformulado a partir dos desafios jurisprudenciais que a corte enfrentou no que tange, por exemplo, à proteção de informações pessoais de acordo com o grau de sigilo do dado, o destinatário da informação, a finalidade da coleta, além do contexto de aplicação daquela informação no caso concreto¹⁰⁶.

A noção de classificação da informação pessoal em níveis de proteção é aprofundada pela Teoria das Esferas de Heinrich Hubmann¹⁰⁷. De acordo com ela, a personalidade do indivíduo poderia ser representada por três esferas concêntricas protegidas em níveis diferentes. A última esfera, que abrange as outras duas, é a esfera individual e social, a qual não estaria protegida pelo direito à privacidade diante da publicidade e ampla divulgação das ações humanas nessa esfera. A esfera do meio seria a esfera da privacidade, que estaria protegida, mas poderia ser restringida diante de interesses específicos. Já a esfera mais interna seria a esfera do sigilo, intocável e, por isso, objeto que não poderia ser violado. No entanto, a Professora Laura Schertel reconhece que a Teoria das Esferas pode ter influenciado a jurisprudência constitucional alemã, mas a corte possuía uma orientação mais funcional sobre o conteúdo a ser protegido pelo direito à privacidade¹⁰⁸.

A privacidade, abarcada pelo direito geral de personalidade, foi reconhecida como objeto de proteção constitucional no julgamento do caso Lebach, ocorrido em 1973. Nesse julgamento, ficou consolidada “a proteção da esfera privada, específica por âmbitos de aplicação, para um direito de personalidade geral e abstrato”¹⁰⁹. Este caso foi julgado pela Corte Constitucional da Alemanha e tinha como objeto analisar a legalidade da transmissão de

¹⁰⁵ MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 216.

¹⁰⁶ MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 222.

¹⁰⁷ HUBMANN Heinrich. **Das Persönlichkeitsrecht**. 2. ed. Colônia: 1967.

¹⁰⁸ MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 221.

¹⁰⁹ MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 224.

um documentário em um canal de televisão sobre um crime cometido à época, citando inclusive o nome e aspectos da personalidade das pessoas condenadas pela autoria do crime. A corte explicou que a transmissão do documentário possui efeitos no âmbito do direito fundamental à personalidade dos envolvidos. Também observou que o direito ao livre desenvolvimento da personalidade e da dignidade humana busca proteger a esfera de autonomia dos indivíduos, inclusive o direito de ‘ser deixado só’ e ‘ser você mesmo’, excluindo a intrusão de outros sobre aspectos da personalidade. A corte enfatizou que tal direito implica, em princípio, a possibilidade de os indivíduos determinarem a si mesmos, se e em que medida outros podem representar publicamente um relato de sua vida¹¹⁰.

Ao mesmo tempo, a vida privada não é objeto de proteção absoluta, principalmente, em vista do escopo e proporcionalidade de um interesse social. Apesar disso, no caso concreto, o interesse social e o direito de informação teriam sido satisfeitos com a persecução penal dos culpados, de forma a justificar a proteção do direito de personalidade. Assim, a corte reconheceu a proteção da privacidade enquanto uma das facetas do direito de personalidade, protegido constitucionalmente¹¹¹. A jurisprudência alemã, apesar da falta de previsão expressa no texto constitucional, passou a reconhecer o direito geral de personalidade como garantia constitucional, que não se esgotava na seara infraconstitucional do Código Civil alemão.

Dessa forma, o desenvolvimento do direito à autodeterminação informativa enquanto direito de personalidade se deu em acordo com a necessidade de soluções judiciais a casos concretos. Os casos levados ao judiciário alemão tencionavam a existência de um direito de privacidade dos indivíduos em relação à terceiros, bem como a possibilidade de controle desses indivíduos sobre seus próprios dados pessoais. Segundo a corte, a construção de um direito geral de personalidade é baseada na ideia de autodeterminação, que significa justamente o direito do indivíduo escolher de que forma quer se apresentar a outras pessoas e, com isso, dispor da sua personalidade.

O Tribunal Constitucional Alemão, no julgamento do caso Eppler, afirmou que “o indivíduo deve ser capaz de decidir por si mesmo, sem restrição a sua esfera privada, como ele quer se apresentar a terceiros ou ao público, se e até que ponto terceiros podem dispor de sua personalidade”¹¹². Assim, a partir de situações concretas e não uniformes, a corte

¹¹⁰ COLUMBIA UNIVERSITY. **The Case of Lebach**. s.d. Disponível em: <https://globalfreedomofexpression.columbia.edu/cases/the-case-of-lebach/>. Acesso em: 26 jan. 2023.

¹¹¹ COLUMBIA UNIVERSITY. **The Case of Lebach**. s.d. Disponível em: <https://globalfreedomofexpression.columbia.edu/cases/the-case-of-lebach/>. Acesso em: 26 jan. 2023.

¹¹² ALEMANHA. Entscheidungen der amtlichen Sammlung 54, 148 (155), **Eppler**. Disponível em: <https://www.servat.unibe.ch/dfr/bv054148.html>. Acesso em: 10 nov. 2022.

constitucional percebeu a necessidade de se garantir proteção constitucional a um direito geral de personalidade de formulação indefinida e abstrata para enfrentar riscos desconhecidos e imprevisíveis à sociedade¹¹³.

A corte constitucional alemã, ao julgar o caso do Recenseamento, identificou um novo desdobramento do direito geral de personalidade, o direito à autodeterminação informativa. Na concepção constitucional alemã, este direito, assim como aquele, não possui um teor de proteção rígido e definido *a priori*, ao contrário da concepção tradicional de privacidade, que não inclui no seu escopo de proteção a dados públicos. Ainda, esse direito garante ao indivíduo poder de decisão sobre como suas informações pessoais serão utilizadas por terceiros, que, necessariamente, são objeto de proteção jurídica, independentemente se considerados relevantes ou não¹¹⁴.

Nos contornos da época, o direito à autodeterminação informativa tinha como objetivo garantir que o titular tivesse liberdade de decidir sobre quais informações pessoais seriam conhecidas por terceiros, bem como a finalidade e demais circunstâncias do uso daquela informação. O processamento eletrônico de dados ampliou sobremaneira as formas de acesso e transmissão de dados, de modo a aumentar a capacidade de influência sobre o comportamento do titular afetado e, com isso, minimizar sua autonomia. Assim, a ideia de que não existe dado insignificante ganha centralidade no âmbito de proteção do direito geral de personalidade, que não se limita aos dados íntimos ou privados, mas a todos aqueles que permitem a identificação de uma pessoa. Em vista de desafios jurídicos concretos no Brasil, esses argumentos foram também desenvolvidos para balizar casos de uso de dados pessoais, que não são irrelevantes, de consumidores, usuários da internet, bem como cidadãos amplamente considerados.

3.2. A autodeterminação informativa no Brasil

A mudança no sentido de um direito à privacidade estava sendo formulada nos EUA, e a sua transição para ideia de autodeterminação informativa foi consolidada na decisão de 1983 do Tribunal Alemão. Essa decisão cunhou o termo da autodeterminação como forma de mitigar os riscos aos direitos de personalidade causados pela disseminação de novas

¹¹³ MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 225.

¹¹⁴ MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 232.

tecnologias que amplificam o poder de processamento de informações. A autodeterminação logo foi entendida como uma nova faceta do direito de personalidade enquanto mecanismo de controle às pessoas em determinarem a informação que terceiros conhecerão sobre elas e como poderão ser utilizadas.

Tendo em vista o objetivo das leis de proteção de dados, a autodeterminação informativa se mostra resultado da garantia do atendimento das legítimas expectativas dos titulares e do livre desenvolvimento da sua personalidade¹¹⁵. Nesse sentido, foram desenvolvidos modelos regulatórios eficazes na proteção desse conceito por meio de mecanismos específicos e replicáveis em outros contextos. O fluxo de dados na sociedade da informação avança para além das fronteiras de território e jurisdição comumente estabelecidas.

Até 2023, mais de 100 países já aprovaram normas gerais sobre privacidade e tratamento de dados pessoais e muitas delas seguem o modelo europeu do RGPD para regular o tema¹¹⁶. O RGPD possui um impacto ao redor do mundo para definição de parâmetros na regulação do tema, seja para aproximar os países dos elementos elencados na União Europeia para proteção de dados pessoais, seja para se afastar desses requisitos¹¹⁷. Alguns dos elementos pensados para a garantia da proteção de dados foram (i) a delimitação da finalidade do tratamento do dado pessoal; (ii) a especificação de uma hipótese legal que fundamentasse o tratamento; (iii) o estabelecimento de um nível de informação adequado a ser transmitido ao titular; (iv) bem como a garantia de direitos ao titular; e (v) o estabelecimento de uma autoridade garantidora do direito.

No Brasil, a LGPD é a lei infraconstitucional a regular a matéria. Ela teve um longo trâmite no Poder Executivo e Legislativo e, por fim, reconheceu como um de seus fundamentos a autodeterminação informativa. Posteriormente à promulgação da lei, em 2018, o Supremo Tribunal Federal (STF), em caso concreto, analisou a incidência desse conceito do ponto de vista constitucional. O caso versava sobre os direitos fundamentais dos cidadãos remontando o contexto da decisão alemã sobre a intrusividade do Estado na gestão de

¹¹⁵ BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 107 (item 2.5)

¹¹⁶ DLA PIPER. **Data Protection Laws of the World**. 2022. Disponível em: <https://www.dlapiperdataprotection.com/>. Acesso: 15 jul. 2022.

¹¹⁷ Para mais informações a título comparativo do RGPD com outras leis de proteção de dados, acesse: GREENLEAF, Graham; COTTIER, Bertil. 2020 Ends a Decade of 62 New Data Privacy Laws. **163 Privacy Laws & Business International Report 24-26**. 2020. Disponível em: <https://deliverypdf.ssrn.com/delivery.php?ID=527000067124025069095112078067099108039003024042071075093075112088116126097095002067114102007027106035006118101120066003025084005082039040022083030076122096006008064047024093092031069065113120083080117087014081023065111025111126073009092030007102&EXT=pdf&INDEX=TRUE>. Acesso em: 14 nov. 2022.

informações pessoais de seus cidadãos. Porém, antes mesmo da promulgação da LGPD e da decisão do STF, o Superior Tribunal de Justiça (STJ) havia percebido a necessidade de proteção da autodeterminação informativa na relação consumerista. Neste item, será apresentado o surgimento da autodeterminação informativa enquanto fundamento da LGPD, suas consequências, bem como a leitura constitucional do conceito no ordenamento jurídico brasileiro feito pelo STF.

3.2.1. A autodeterminação informativa enquanto fundamento da proteção de dados nas normas brasileiras

A autodeterminação informativa, enquanto motor para autonomia do titular em decidir sobre como suas informações serão tratadas por terceiros, já poderia ser deduzida do ordenamento jurídico brasileiro a partir de previsões esparsas. Desde a promulgação da Constituição de 1988, no art. 5º, LXXII, está prevista a ação de *Habeas Data*. Por meio dessa ação, o titular de dados tem o direito de conhecer ou de retificar as suas informações pessoais constante em registros ou bancos de dados de entidades governamentais ou de caráter público. Essa ação é mecanismo assegurado ao titular de dados para que ele possa saber e corrigir as suas informações pessoais conhecidas pelo Poder Público, garantindo uma gerência mínima sobre esses dados.

A respeito do momento de discussão sobre a positivação dessa ação na Constituição de 1988, Danilo Doneda destaca que a noção de liberdade informática teria inspirado o constituinte na elaboração do *Habeas Data*. Segundo o autor, essa ação era percebida “como uma extensão da liberdade pessoal como consequência necessária do desenvolvimento tecnológico, aludindo inclusive à importância do *habeas corpus*, estrutura na qual o *habeas data* foi inspirado, para a liberdade pessoal”. No entanto, esta ação não avançou, em termos práticos, o debate sobre dados pessoais¹¹⁸. Ainda, o art. 5º, X e XII, protege a autodeterminação ao prever a inviolabilidade da intimidade e da vida privada, além do sigilo dos dados e comunicações, cabendo ao indivíduo controlar de que forma seus dados poderão ser utilizados. Como evidenciado anteriormente (tópico 1), desde 2022, a proteção de dados passou a constar explicitamente no rol de direitos fundamentais da Constituição.

O CDC (Lei 8.078/1990), em seu art. 43, garante ao consumidor o direito de informação sobre a existência de banco de dados com suas informações pessoais e o direito de

¹¹⁸ DONEDA, Danilo A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. CUEVA, Ricardo Villas Bôas Cueva; DONEDA, Danilo; MENDES, Laura Schertel (coord.). **Lei geral de proteção de dados** (Lei nº 13.709/2018): a caminho da efetividade, contribuições para a implementação da LGPD. 1. ed. São Paulo: Thomson Reuters Brasil, 2020, p. RB-15.1.

acesso aos dados registrados e as fontes de informação de forma acessível. O art. 6º, II, prevê ser direito básico do consumidor receber informações adequadas e claras sobre os produtos e serviços, especificamente sobre suas características e riscos. Ainda, é garantido o direito de retificação dos dados quando estiverem inexatos, que, em conjunto com as previsões expressas anteriormente, garante ao consumidor, na condição de titular de dados, o controle sobre suas informações armazenadas em arquivos relacionados a consumo¹¹⁹.

A LCP (Lei nº 12.414/2011) dispõe sobre a formação de bancos de dados com informações de adimplemento de crédito. Ela determina, em seu art. 5º, que a pessoa cadastrada poderá (i) solicitar cancelamento do cadastro; (ii) impugnar informações errôneas anotadas no banco; (iii) ter seus dados tratados apenas para finalidade da coleta; (iv) conhecer os critérios utilizados para análise de risco de crédito; (v) solicitar revisão de decisão realizada exclusivamente por meios automatizados. Esses direitos dialogam diretamente com a pretensão do titular em decidir com liberdade sobre como seus dados serão tratados, apesar da existência de outras lacunas que garantam a autodeterminação nesta lei. A Lei Complementar nº 166, de 2019, alterou sobremaneira os dispositivos da Lei do Cadastro Positivo mitigando outros elementos relacionados com uma autodeterminação informativa. A título de exemplo, antes da aprovação desta Lei Complementar, cabia ao cadastrado, titular de dados pessoais, autorizar previamente ao cadastro, mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada, a sua inscrição no cadastro positivo. Esse dispositivo garantia autonomia ao titular em decidir se quer ou não ter seus dados tratados neste contexto, porém sua redação foi alterada.

Já a LAI (Lei nº 12.527/2011) apresenta uma série de mecanismos para que as pessoas possam acessar de maneira facilitada informações conhecidas e processadas pelo Poder Público. O Estado também é responsável por diversos tratamento de dados, inclusive pessoais, e diante dos princípios republicanos de transparência e publicidade, deve garantir nível robusto de informação disponível para seus cidadãos, seja para fiscalizar a atuação estatal, seja para atender o seu direito fundamental de acesso à informação (art. 5º, XXXIII, da CF). Ao mesmo tempo, cabe ao Poder Público garantir respeito às liberdades e garantias individuais, mesmo daqueles que se relacionam com o Estado e podem ser expostos pelo dever de transparência. Nesse sentido, o art. 31 da lei apresenta parâmetros para solução desse aparente conflito entre publicidade e privacidade por meio da restrição de acesso a

¹¹⁹ GAMBOGI, Ana Paula. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (org.). **Coleção doutrinas essenciais**: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 915-954, p. 930.

informações relativas à intimidade, vida privada, honra e imagem do titular, que se relaciona com a capacidade do titular em se autodeterminar.

O MCI (Lei nº 12.965/2014) estabelece a proteção de dados pessoais como princípio do uso da internet no Brasil. A lei também prevê os direitos relacionados ao acesso à internet, como o direito de informação sobre o tratamento de dados pessoais. Desde o MCI, os dados pessoais só poderiam ser utilizados para finalidade legal, que justifica a coleta, e especificada nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. Pelo MCI, o usuário teria de consentir expressamente e de forma destacada sobre o tratamento de seus dados pessoais, além de poder solicitar a exclusão definitiva de suas informações no término da relação entre o usuário e o provedor de aplicação de internet. Percebe-se que as normas do Marco Civil “desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento”¹²⁰. No MCI, o consentimento é escolhido como forma de garantia da autodeterminação do usuário, no entanto, como será visto a seguir, esse elemento não é a única forma de se garantir observância a este fundamento.

Já em uma perspectiva voltada para a proteção de dados, a LGPD foi a primeira regulação que reconheceu a autodeterminação informativa de forma expressa como conceito juridicamente relevante. Essa lei possui um caráter geral, ou seja, é aplicável tanto ao contexto do tratamento de dados realizado pelo Poder Público, quanto por entidades e empresas privadas, de forma a competir a todos esses atores a observância da autodeterminação. Porém, não foi desde o início da concepção da LGPD que esse fundamento esteve previsto, ainda mais podendo ser associado a um direito à explicação em decisões automatizadas baseada em dados. Para entender o desenvolvimento do conceito e de um direito à explicação na LGPD, analisou-se os principais documentos vinculados à concepção da lei e seu trâmite nas duas casas legislativas entre 2010 a 2018, ano de sua promulgação.

O primeiro esboço do que viria a ser a LGPD foi tornado público em novembro de 2010 pelo Ministério da Justiça (MJ) para consulta pública e recebimento de contribuições pela sociedade¹²¹. Essa versão do texto foi inspirada no debate estabelecido no Mercosul sobre uma possível regulação homogênea a respeito do tratamento de dados pessoais no bloco. Antes da divulgação do texto, no mesmo ano, o Subgrupo de Trabalho 13 aprovou o

¹²⁰ BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 128, item 3.3.3.3.

¹²¹ BRASIL. Ministério da Justiça. **Cultura Digital**. 2010. Disponível em: <http://pensando.mj.gov.br/dadospessoais2011/debata-a-norma/>. Acesso em: 14 nov. 2022.

documento “Medidas para a proteção de dados pessoais e sua livre circulação”, mas que não chegou a ser deliberado como normativa do Mercosul pelo Grupo Mercado Comum¹²².

Este documento, assim como a minuta formulada pelo MJ, não previa a autodeterminação como fundamento da lei ou mesmo objeto de proteção jurídica, mas previa hipóteses legitimadoras do tratamento e direitos de acesso, retificação e bloqueio de dados. Especificamente sobre decisões automatizadas, o documento estabelecia que os Estados parte do Mercosul assegurariam que os indivíduos não fossem sujeitos a qualquer decisão a qual produza efeitos jurídicos ou os afete significativamente e se baseie unicamente no tratamento automatizado de dados destinados à sua avaliação. Tal tratamento só seria aceito se a proteção efetiva dos direitos e interesses legítimos do titular fosse garantida por contrato ou por lei¹²³.

Entre 2010 e 2015, novo texto-base foi elaborado pela Secretaria Nacional do Consumidor do MJ como Anteprojeto de Lei de Proteção de Dados. Nesse meio tempo, o deputado federal Milton Monti apresentou o PL nº 4060/2012, para dispor sobre o tratamento de dados pessoais. Em sua forma original, esse PL excluía as ferramentas de proteção de dados pessoais aos dados tratados pela Administração Pública e conceituava dados pessoais como informação precisa sobre pessoa determinada, de forma diversa do que ficou consolidado com a LGPD. O PL estabelece um direito à “autodeterminação das informações e dados pessoais prestados ou coletados, por qualquer meio”, mas não cria direito específico para decisões automatizadas¹²⁴. O PL foi enviado à Comissão de Ciência e Tecnologia, Comunicação e Informática, mas permaneceu adormecido até meados de 2016.

Em 2015, o novo texto do MJ foi tornado público e submetido a escrutínio público, o qual resultou em cerca de 1200 contribuições enviadas por documentos apartados e pela plataforma “Pensando o Direito”¹²⁵. Nessa redação, a autodeterminação informativa continuava a não ser mencionada, mas a forma de regular as decisões automatizadas foi alterada. Passou a estar previsto o dever do responsável pelo tratamento em fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados

¹²² MACEDO, André Batisti de; SCHMIDT, Roberto Eurico. **O Regime de Responsabilidade Civil aplicado na Lei Geral de Proteção de Dados**. [S.l.]. Disponível em:

<https://repositorio.animaeducacao.com.br/bitstream/ANIMA/25299/1/ARTIGO.pdf>. Acesso em: 1 mar. 2023.

¹²³ MERCOSUL. **Protección de datos personales y su libre circulación**. 2010. Disponível em:

https://documentos.mercosur.int/simfiles/proynormativas/24606_SGT13_2010_ACTA01_ANE04_PDecS-N_ES_Protecci%C3%B3n%20Datos%20Personales.pdf. Acesso em: 14 nov. 2022.

¹²⁴ BRASIL. Câmara dos Deputados. **Inteiro Teor PL 40460/2012**. 2012. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012. Acesso em: 14 nov. 2022.

¹²⁵ BRASIL. **Consulta Pública - Anteprojeto de Lei para a Proteção de Dados Pessoais**. Pensando o Direito. 2015. Disponível em:

<http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso: 13 nov. 2022.

para a decisão automatizada. Essa previsão é similar ao texto atual do §1º do art. 20 da LGPD, porém a lei acrescenta a condição do segredo comercial e industrial para esse dever de informação.

A preocupação com o segredo comercial e industrial foi objeto de preocupação de empresas que, na consulta pública em 2015. Esse setor já apontava a possibilidade de um dever de informação sobre os critérios e procedimentos utilizados para a decisão automatizada ferir a liberdade de contratação, o segredo de negócio e facilitaria a prática de infrações penais como a fraude. Isso porque “conhecendo os critérios e procedimentos utilizados pelos sistemas das seguradoras fica muito mais fácil encontrar caminhos para burlar os sistemas de aceitação”. Esses apontamentos foram feitos pela Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações e pela CNseg¹²⁶.

Com as contribuições populares, foi formulado um novo texto para o anteprojeto de lei que, nas vésperas do afastamento da então presidenta Dilma Rousseff, foi encaminhado à Câmara dos Deputados para seguir tramitação legislativa. O texto do Poder Executivo foi transformado no PL nº 5276/2016¹²⁷, que foi apensado ao PL nº 4060/2012, e começaram a tramitar em conjunto, em julho de 2016.

Em sua versão original, o PL nº 5276/2016 previa a autodeterminação informativa como fundamento da proteção de dados. Nas motivações do PL, fica explícito que “a proposta visa assegurar ao cidadão o controle e a titularidade sobre suas informações pessoais, com fundamento na autodeterminação informativa”. Ainda, a garantia dos direitos fundamentais, como o da privacidade, depende “das respostas coletivas que serão apresentadas para implementá-lo, motivo pelo qual é necessário empenhar-se na construção de uma democracia da informação”, que observa a autodeterminação, a liberdade de controle das informações pessoais, e a tutela contra a utilização discriminatória dos dados¹²⁸. Com esse PL, restou consolidado o texto do §1º, do art. 20, sobre o dever do controlador, enquanto responsável pelo tratamento, em informar o titular sobre os critérios e os procedimentos utilizados para a decisão automatizada, respeitados os segredos comercial e industrial.

¹²⁶ BRASIL. **Consulta Pública - Anteprojeto de Lei para a Proteção de Dados Pessoais**. Pensando o Direito. 2015. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso: 13 nov. 2022.

¹²⁷ BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5.276/2016**. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459. Acesso em: 13 nov. 2022.

¹²⁸ BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5.276/2016**. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459. Acesso em: 13 nov. 2022.

Em agosto de 2016, a Mesa da Câmara dos Deputados determinou a criação de uma Comissão Especial para proferir parecer ao PL nº 4060/2012¹²⁹, que tinha a ele apensado o PL nº 6291/2017 e o PL nº 5276/2016. A comissão foi constituída em outubro de 2016 e o PL foi distribuído para o relator Deputado Orlando Silva no mesmo mês. Durante a tramitação do PL e de seus apensados na Comissão, entre os anos de 2016 e 2018, foram aprovados requerimentos para realização de audiências públicas para debate amplo sobre os dispositivos do texto e melhor forma de regular a proteção de dados no Brasil. A tramitação do projeto que deu origem à LGPD é conhecida pela participação de diversos setores da sociedade, como o empresarial, acadêmico, público, técnico e sociedade civil organizada. Esse processo foi determinante para a aprovação do PL por unanimidade no plenário da Câmara.

Em 28 de maio de 2018, o Deputado Orlando Silva apresentou seu parecer pela aprovação do PL na forma do substitutivo. O parecer apresentou um texto substitutivo, o qual manteve a autodeterminação informativa como fundamento da lei e o dever do controlador informar o titular a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial¹³⁰. Para além das questões relacionadas à autodeterminação na decisão automatizada, o parecer é resultado de um trabalho o qual compilou um relatório dos PLs apensados, as emendas apresentadas, o contexto de tramitação da matéria, as principais contribuições feitas em audiência públicas, bem como as modificações introduzidas pelos substitutivo e a justificativa respectiva.

No dia seguinte, o plenário da Câmara dos Deputados discutiu e aprovou o PL, nos termos do relatório do Deputado Orlando Silva, que foi encaminhado ao Senado Federal. Estava em trâmite, no Senado Federal, o PL nº 330/2013, apresentado pelo Senador Antônio Carlos Valadares, que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais. Esse PL não cita a autodeterminação informativa e não prevê critérios específicos para decisão automatizada, mas garante direitos ao titular de dados de acesso aos bancos de dados, ciência no momento da inscrição e retificação do dado inexato. O PL foi julgado prejudicado em virtude da deliberação do Projeto de Lei Complementar nº 53/2018¹³¹.

Nesta casa, o PL foi analisado pela Comissão de Assuntos Econômicos, que aprovou relatório do Senador Ricardo Ferraço, pela aprovação do PL com emendas, sem alteração

¹²⁹ BRASIL. Câmara dos Deputados. **Requerimento n. 5.017/2016**. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1484640. Acesso em: 14 nov. 2022.

¹³⁰ BRASIL. Câmara dos Deputados. **Comissão especial destinada a proferir parecer ao projeto de lei nº 4060, de 2012**. 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305. Acesso em: 14 nov. 2022.

¹³¹ Para mais informações, acesse: <https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pls-330-2013>.

substancial da matéria da lei¹³². O texto também foi aprovado pela Comissão de Ciência, Tecnologia e da Comissão de Justiça do Senado. Ainda, a Comissão Diretora, em plenário, apresentou a redação final do PL para adequar o texto à técnica legislativa pertinente. Com isso, o PL nº 4060/2012 seguiu para sanção presidencial, proferida no dia 14 de agosto de 2018, com vetos¹³³. Em resumo, é possível estabelecer a seguinte linha do tempo:

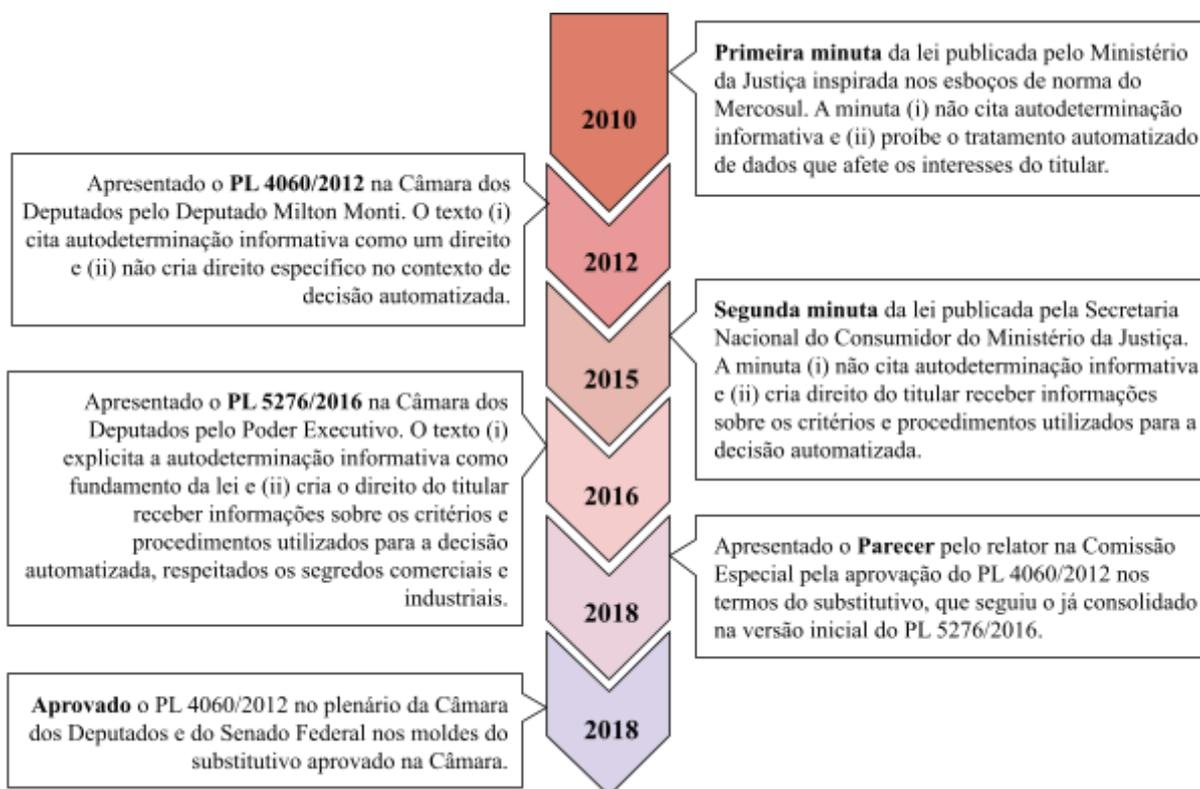


Figura 5 - Linha do tempo sobre a autodeterminação e decisão automatizada no projeto de lei da LGPD

Em vista de uma análise sobre a tramitação da LGPD nas casas do Legislativo, o conceito da autodeterminação informativa, apesar de central no desenvolvimento da matéria de proteção de dados, não estava previsto desde as primeiras formulações do que viria a ser a LGPD. Ao mesmo tempo, com a sua inclusão no texto em 2016, o conceito não foi objeto de controvérsia ou discussão pelos agentes interessados, ao contrário da regulamentação da decisão automatizada baseada em dados pessoais. Inicialmente, a primeira minuta de lei estabelecia a impossibilidade de tratar dados de forma automatizada que afetasse os interesses do titular. Essa previsão foi substituída pelo estabelecimento do dever do controlador informar

¹³² BRASIL. Senado Federal. **Relatório legislativo CAE**. 2018. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7751914&ts=1630450894215>. Acesso em: 14 nov. 2022.

¹³³ BRASIL. Presidência da República. **Mensagem nº 451, de 14 de agosto de 2018**. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 14 nov. 2022. Todos os vetos foram mantidos pelo Congresso Nacional.

o titular sobre os critérios e procedimentos utilizados para a tomada de decisão. Essa mudança não foi especificamente justificada nos relatórios de tramitação do PL, que seguiu e foi aprovada pelo Congresso, modificada apenas para acrescentar a observância do segredo comercial e industrial, na efetivação do direito à explicação do titular, como será analisado mais adiante nesta pesquisa (tópico 5).

3.2.2. A autodeterminação informativa enquanto conceito base para decisão do Supremo Tribunal Federal

O conceito da autodeterminação informativa foi cunhado pelo STF no acórdão de julgamento das Ações Diretas de Inconstitucionalidade 6387, 6388, 6389, 6390, 6393, em maio de 2020¹³⁴. Nessa oportunidade, o STF reconheceu um direito fundamental à proteção de dados autônomo da privacidade e protegido pelos fundamentos constitucionais. Essas ações tinham como objeto a inconstitucionalidade da Medida Provisória (MP) 954, de abril de 2020. A MP previa o compartilhamento de dados dos usuários do Serviço Telefônico Fixo Comutado e do Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatística oficial durante a pandemia do coronavírus. Os propositores das ações argumentaram que o compartilhamento de nome, número de telefone e endereço dos usuários violaria o direito constitucional à intimidade, à vida privada e ao sigilo de dados.

No mesmo mês que a MP foi publicada e as ações foram propostas, a Ministra relatora Rosa Weber deferiu a medida cautelar requerida para suspender a eficácia da MP e determinar que o IBGE se abstenha de requerer dados com base nessa medida às empresas de telecomunicações, diante de sua inconstitucionalidade. Em maio de 2020, a medida foi referendada no plenário em acórdão o qual analisou a possível violação de direito material causada pela MP em questão e marcou a evolução da matéria de proteção de dados e do conceito da autodeterminação informativa no âmbito jurisprudencial.

O julgamento não foi unânime. O Ministro Marco Aurélio divergiu da tese defendida pela Ministra relatora e defendeu a constitucionalidade da MP. Para o Ministro, as limitações de compartilhamento de dados previstas na MP eram adequadas e suficientes para proteção dos direitos fundamentais. O ministro destacou as medidas de balizamento temporal de eficácia da MP à situação de emergência da pandemia e a definição de finalidade exclusiva de

¹³⁴ BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022.

uso dos dados para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Os outros ministros, Celso de Mello, Edson Fachin, Ricardo Lewandowski, Cármen Lúcia, Dias Toffoli, Luiz Fux, Roberto Barroso, e Gilmar Mendes acompanharam a relatora pela inconstitucionalidade da MP.

Na ementa, o plenário acordou que o tratamento de dados pessoais deve observar os limites constitucionais da liberdade individual (art. 5º, caput, CF), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII, CF), sob pena de lesão a esses direitos. Por isso, qualquer tratamento de dados pelo Poder Público, inclusive de compartilhamento, deve garantir a proteção e a segurança daquelas informações. Com base nessas condições e na necessidade, adequação e proporcionalidade da MP, o STF entendeu que a medida provisória não atende um interesse público legítimo de forma suficientemente clara a qual autorizaria o compartilhamento de dados dos usuários.

Em seu voto, a Ministra Rosa Weber destaca que o compartilhamento de dados, nos moldes determinados pela MP, é excessivo e desproporcional, tanto pela quantidade de titulares afetados, quanto pela amplitude da finalidade do tratamento de dados, que era genericamente previsto como produção estatística oficial. Um ponto de atenção seria os riscos e possíveis efeitos danosos do processamento dessas informações em outros contextos. Nesse sentido, as antigas listas telefônicas disponibilizadas ao público com nome, telefone e endereço dos assinantes não se comparam com o que pode ser feito com essas informações a nível de processamento, cruzamento e filtragem de dados para formação de perfis do titular.

Em acordo com esses argumentos, o Ministro Luiz Fux entende que a MP (i) não delimita para quais finalidades os dados serão utilizados; (ii) não especifica os procedimentos de segurança para evitar vazamento de dados; (iii) determina a elaboração de um relatório de impacto à proteção de dados após o compartilhamento, porém a elaboração deve ser anterior a esse tratamento para garantir transparência e permitir aferição dos riscos; e (iv) permite tratamento de dados o qual pode gerar um nível alto de precisão na identificação e formação de perfil dos usuários.

A análise dos ministros sobre os possíveis usos dos dados pessoais compartilhados para finalidade e sobre o escopo de proteções diferentes dialoga diretamente com a capacidade do indivíduo em se autodeterminar. Isso porque, diante de uma MP não precisa sobre os parâmetros de proteção de dados, o titular não teria controle sobre o uso de suas informações pessoais ou mesmo instrumentos que o colocassem em posição de destaque com direitos e proteções específicas. Isso demonstra a fragilidade da MP em garantir observância

aos padrões mínimos de proteção de dados, especialmente ao atingimento dos princípios de finalidade, necessidade e adequação no compartilhamento dos dados com o IBGE.

O Ministro Gilmar Mendes reconhece o direito à proteção de dados apartado de um direito à privacidade e ao sigilo, direitos fundamentais consolidados e mais aplicados pela jurisprudência no contexto de acesso à informação. Para tanto, o ministro relembra o julgamento alemão sobre a Lei do Censo, em que a corte constitucional alemã redefiniu as delimitações e sentidos de um direito à proteção de dados pessoais como projeção do direito geral de personalidade, o qual não se resume a uma proteção constitucional do sigilo. Na leitura do ministro, o tribunal alemão entendeu que o processamento automatizado de dados “colocaria em risco o poder do indivíduo de decidir por si mesmo sobre se e como ele desejaria fornecer a terceiros os seus dados pessoais”¹³⁵. Assim, o tribunal, na época, buscou evitar um cenário em que, por meio do processamento de dados, as informações fornecidas pelos cidadãos fossem tratadas de modo a formar um perfil completo da personalidade do cidadão submetido ao censo. Essa preocupação, como destacado anteriormente, está relacionada a uma ideia de autodeterminação.

Desde a decisão a qual concedeu a medida liminar, a ministra relatora reconheceu o direito fundamental à autodeterminação informativa, de forma a ser necessária uma tutela jurisdicional quando a mitigação desse direito não for motivada por razões suficientes, proporcionais, necessárias e adequadas. De forma similar, o Ministro Luiz Fux entende ser a autodeterminação informativa um direito autônomo extraído “da garantia da inviolabilidade da intimidade e da vida privada e, conseqüentemente, do princípio da dignidade da pessoa humana”¹³⁶. O direito à autodeterminação seria necessário para que o indivíduo desenvolva livremente sua personalidade, o qual, no caso concreto, não estaria devidamente protegido pela MP. Há lacuna, no texto da medida, sobre a “transparência e informação necessários para uma adequada composição e conciliação entre a necessidade de produção estatística e os direitos fundamentais à proteção de dados e à autodeterminação informativa”¹³⁷.

É nesse sentido que, para o Ministro Gilmar Mendes, a autodeterminação seria uma relevante chave interpretativa para a garantia do direito à proteção de dados pessoais. O objeto

¹³⁵ BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022, p. 101

¹³⁶ BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022, p. 49

¹³⁷ BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022, p. 67

da proteção não se limita àquelas informações privadas, mas abrange os riscos atribuídos ao tratamento de dados por terceiros, mesmo quando públicos¹³⁸. A dimensão subjetiva desse direito indica que a intervenção do Estado no campo da informação pessoal só seria legítima a partir da identificação feita pelo legislador de justificativas constitucionais com finalidade e limite específico. Já a dimensão objetiva impõe que o legislador garanta a proteção de dados a partir de mecanismos institucionais de salvaguarda traduzidos em normas de organização, procedimento e proteção¹³⁹.

Portanto, o STF reconheceu a existência de um direito à proteção de dados a ser protegido por meio da fixação de salvaguardas mínimas e suficientes para a garantia dos direitos fundamentais e da dignidade humana. Para o plenário, essas garantias não estavam previstas na MP e não haveria um interesse público legítimo no compartilhamento dos dados pessoais dos usuários, de forma a não ser juridicamente adequado endossar o texto da MP. Em outubro de 2020, as ADIs foram julgadas prejudicadas por perda superveniente do objeto, em vista da não aprovação da MP pelo Congresso Nacional, que a transformaria em lei.

Anos antes da promulgação da LGPD e da decisão do STF, o STJ já havia enfrentado questões que indicavam para necessidade de tutela jurisdicional a um direito à autodeterminação informativa no âmbito consumerista. Com base no CDC, de 1990, o tribunal superior já havia reconhecido a emergência de um novo significado para o direito de privacidade, que, tradicionalmente, se restringia à objeção da interferência de terceiros¹⁴⁰. De acordo com esse novo sentido, o direito fundamental à privacidade ganhou uma dimensão de controle, com o desenvolvimento da tecnologia, em que para tutelar a privacidade, passava a ser necessário que o titular pudesse dispor com exclusividade sobre seus dados pessoais¹⁴¹. Essa interpretação e a consolidação de uma jurisprudência alinhada a um novo sentido para a privacidade surgiram com as lides a respeito de abusos na coleta e no tratamento de dados pessoais em bancos de dados e cadastros de consumidores com informações de crédito. Na

¹³⁸BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022, p. 103

¹³⁹BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022, p. 109

¹⁴⁰ CUEVA, Ricardo Villas Bôas. Banco de dados e cadastros de consumidores no Código de Defesa do Consumidor: da privacidade à proteção de dados pessoais. **Revista do Advogado**, ano XL, n. 147, setembro de 2020, p. 96.

¹⁴¹ BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.168.547/RJ**. Relator Ministro Luis Felipe Salomão. 2010. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=959347&num_registro=200702529083&data=20110207&formato=PDF. Acesso em: 16 nov. 2022, p. 2

época, esses cadastros começavam a surgir como ferramenta de registro e proteção ao crédito, mas que deveriam observar o direito de acesso e retificação dos dados pessoais, como determina o art. 43 do CDC.

3.3. Síntese preliminar da aplicação da autodeterminação informativa na regulação de proteção de dados

Diante de uma concepção de autodeterminação informativa enquanto fundamento jurídico na decisão alemã, com sentido brasileiro preenchido na tramitação da LGPD, e na decisão do STF, é possível depreender que o ordenamento jurídico visa proteger o tratamento de dados pessoais contra potenciais riscos de violação de direitos. Destaca-se, principalmente, os direitos da dignidade da pessoa humana e da privacidade, em um contexto de elevado poder computacional para processamento de dados. A autodeterminação é um dos fundamentos dessa proteção jurídica, já que visa garantir o livre desenvolvimento da pessoa em acordo com sua subjetividade e autonomia em se determinar perante terceiros.

Para tanto, uma possível forma de garantir essa capacidade do indivíduo se autodeterminar é assegurar a ele mecanismos de controle sobre sua informação pessoal, seja limitando o acesso a terceiro, seja especificando a forma de tratamento desse dado. Essa ideia de autodeterminação informativa é bastante semelhante ao que Daniel Solove chama de *privacy self-management*. Esse conceito aponta para a ideia de fornecer às pessoas controle sobre seus dados pessoais e, por meio desse controle, as pessoas poderiam decidir por si mesmas como avaliar os custos e benefícios da coleta, uso ou divulgação de suas informações pessoais¹⁴².

No contexto alemão, a autodeterminação informativa foi resultado de uma interpretação do texto constitucional que garante o livre desenvolvimento da personalidade e a dignidade humana. Com isso, foi fixado um direito geral de personalidade amplo e flexível que concebe de forma abstrata o direito da pessoa autodeterminar-se. Essa percepção se afasta de um direito de ação, por este não proteger o indivíduo da intrusão de terceiros, e do conceito tradicional da privacidade, por ter como objeto de proteção apenas aquilo que não é público¹⁴³. Ao mesmo tempo, a autodeterminação informativa assume característica de

¹⁴² SOLOVE, Daniel. Privacy Self-Management and the consent Dilemma. **Harvard Law Review**, v. 126, 2013, p. 1880.

¹⁴³ MENDES, Laura Schertel. 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/view/10828/pdf>. Acesso em: 16 nov. 2022, p. 15.

adaptabilidade em que o indivíduo passa a exercer poder de decisão no tratamento de dados pessoais¹⁴⁴.

Na tentativa de diferenciar o direito de proteção de dados e a autodeterminação informativa, o ordenamento jurídico brasileiro positivou expressamente um direito à proteção de dados como direito fundamental constitucional (art. 5º, LXXIX), enquanto que a autodeterminação informativa seria fundamento para alcançar esse direito. Do ponto de vista doutrinário, a proteção de dados seria uma garantia procedimental do exercício da autodeterminação, conceito mais próximo a uma garantia material do livre desenvolvimento da personalidade. Dessa forma, não há sobreposição entre os objetos do direito à proteção de dados, amplo e procedimental, e à autodeterminação informativa. Esta é “precondição para uma ordem comunicacional livre e democrática” e se ocupa a garantir a possibilidade das pessoas decidirem autonomamente sobre o acesso, uso e difusão de seus dados pessoais¹⁴⁵.

Ainda, o Ministro Gilmar Mendes, no seu voto para referendar a medida cautelar na ADI 6.388, entendeu ser o direito à privacidade uma manifestação do direito à autodeterminação informativa. Este direito seria concretamente garantido a partir de um teste de proporcionalidade para avaliação da adequação, necessidade e proporcionalidade em sentido estrito, como formulado por Alexy¹⁴⁶, modelo levado em consideração no julgamento da corte alemã de 1983¹⁴⁷. De forma complementar, Bruno Bioni nota que a “própria intelecção da proteção de dados pessoais foi forjada sob a alcunha de autodeterminação”¹⁴⁸.

Em um primeiro momento, a concretude da autodeterminação foi reduzida à coleta do consentimento do titular que, apenas assim, poderia controlar de forma autônoma seus dados pessoais. Essa noção evidencia uma certa centralidade do consentimento na regulação de dados pessoais, isso porque o legislador se ocupa a qualificar o consentimento e efetivar os

¹⁴⁴ MENDES, Laura Schertel. 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/view/10828/pdf>. Acesso em: 16 nov. 2022, p. 15.

¹⁴⁵ SARLET, Ingo W.; DONEDA, Danilo; MENDES, Laura S. **Estudos sobre proteção de dados pessoais. (Coleção Direito, tecnologia, inovação e proteção de dados num mundo em transformação)**. São Paulo: Editora Saraiva, 2022, p. 23.

¹⁴⁶ MARTINS, Alessandra Ferreira. **Exame de proporcionalidade nos casos de colisão de direitos fundamentais**. Monografia (Graduação) - Faculdade de Direito da Universidade Federal do Paraná, 2003, p. 49. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/44913/M221.pdf?sequence=1&isAllowed=y>. Acesso: 10 nov. 2022.

¹⁴⁷ BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022, p. 113

¹⁴⁸ BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 133, item 3.4.

adjetivos da sua definição por meio de instrumentos formais e específicos¹⁴⁹. O consentimento está relacionado aos contornos negociais induzidos no tratamento de dados, em que o titular exerceria seu direito de propriedade para negociar a transferência ou não de informações pessoais¹⁵⁰. Essa noção negocial do dado enquanto um objeto de propriedade do titular e não um elemento de sua personalidade é criticada e foi superada em diversos modelos de regulação, em que a proteção de dados é apresentada enquanto direito fundamental e não instrumento de negociação com terceiros¹⁵¹.

Porém, com o passar do tempo, percebeu-se que a autodeterminação não é concretizada apenas pela verificação formal do consentimento do titular. Ou seja, a ciência e a autorização qualificada do titular de dados não é suficiente ou única forma de observância da capacidade do indivíduo se autodeterminar a partir de seus dados pessoais para com terceiros. Veridiana Alimonti especifica que o fluxo de dados “não depende necessariamente da capacidade do indivíduo de controlá-lo desde o início. Refere-se à sua compatibilidade com disciplina de proteção mais abrangente que estabelece princípios, limites e instrumentos que atentam à perspectiva individual, mas que vão além”¹⁵².

É nessa perspectiva que esta pesquisa analisa a conformidade do tratamento de dados pessoais em decisões automatizadas. Baseia-se na noção de autodeterminação informativa por meio do direito à explicação, já que a LGPD estabelece mecanismos para além do consentimento para a garantia da autodeterminação. A LGPD é resultado desse amadurecimento da função do consentimento na proteção de dados, já que reconhece diversos outros cenários nos quais a autodeterminação do titular pode ser respeitada. Isso mesmo quando ele não tiver consentido com o tratamento o qual está exposto, como o cumprimento de obrigação legal, a execução de políticas públicas e o legítimo interesse.

Para outros autores, a autodeterminação também é composta por elementos substanciais de identificação de riscos concretos à liberdade do indivíduo e limites materiais do tratamento de informações pessoais, além da garantia de um poder de decisão formal e

¹⁴⁹ BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 114, item 3.2.

¹⁵⁰ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Revista dos Tribunais, 2019, p. 198. ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. RB-11.2.

¹⁵¹ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Revista dos Tribunais, 2019, p. 198.

¹⁵² ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. RB-11.2.

instrumentos procedimentais para tanto¹⁵³. Nesse sentido, o nível de atendimento do requisito da autodeterminação informativa enquanto fundamento da matéria de proteção de dados seria determinado pela capacidade do indivíduo participar do tratamento de suas informações pessoais. Veridiana Alimonti identifica dois movimentos complementares para se alcançar alguma participação nesse processo: individual, ampliando o poder de barganha do titular com o agente de tratamento, e, estrutural, promovendo padrões de proteção que se aplicam ao coletivo de titulares, sem haver necessidade do engajamento individual¹⁵⁴.

Tradicionalmente associada ao aspecto de controle individual sobre dados pessoais, a autodeterminação vai além da possibilidade de reconhecer o titular de dados como mero fornecedor de informações sobre si e seu contexto em contrapartida ao acesso a bens, serviços, políticas públicas e benefícios sociais. Para Rodotà, cabe ao titular exercer controle direto sobre a forma de processamento de suas informações pessoais, que é feito por agentes os quais adquirem poder a partir dessa atividade. Isso quer dizer que “a possibilidade de controlar não serve apenas para assegurar ao cidadão a exatidão e o uso correto das informações a ele diretamente relacionadas, mas pode se tornar um instrumento de equilíbrio na nova distribuição de poder que vai se delineando”¹⁵⁵.

Esse sentido complementar atribuído à autodeterminação é potente por direcionar novos olhares sobre o objetivo de se regular a proteção de dados e, com isso, sobre as ferramentas que devem ser elaboradas para se alcançar essa redistribuição de poder por meio do controle efetivo sobre os dados pessoais. É relevante notar que, para Rodotà o controle individual poderia ser considerado uma contradição em termos, diante da falta de poder do indivíduo se opor ao tratamento de dados realizado por empresas privadas ou pelo Estado. Assim, a noção de controle relacionada à autodeterminação informativa não se esgotaria no exercício de um controle individual pelo titular como um fim em si mesmo, mas como uma ferramenta de realocação de poder na sociedade. Rodotà destaca a importância do coletivo para a proteção de dados pessoais para além das fronteiras do indivíduo como centro da privacidade. Para o autor,

[r]aramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios

¹⁵³MENDES, Laura Schertel. 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/view/10828/pdf>. Acesso em: 16 nov. 2022, p. 16.

¹⁵⁴ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. RB-11.2.

¹⁵⁵RODOTÀ, Stefano. **A vida na sociedade da vigilância**. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em "controle". Aliás, a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejoso de esquivar-se dos novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de um jogo do qual somente poderá sair como perdedor¹⁵⁶.

A professora Claudia Quelle¹⁵⁷ entende que a autodeterminação informativa visa proteger indiretamente a capacidade dos indivíduos definirem, por si mesmos, quais são seus interesses e necessidades e como eles devem ser protegidos em uma sociedade justa. Dessa forma, a autodeterminação teria como objeto um poder político de determinar o que significa possuir direitos fundamentais em um contexto. Por exemplo, se o Estado está ciente das reuniões de um grupo político controverso, ele está em posição de proibir fundamentalmente essa reunião, determinando assim que ela não é digna de proteção sob os direitos e liberdades fundamentais relevantes. Da mesma forma, uma pessoa pode desejar ocultar informações sensíveis sobre si mesma em contextos específicos, a fim de impedir que outros a discriminem com base nessas informações, protegendo assim seu direito à igualdade de tratamento. Sua capacidade de controlar se a informação sensível é conhecida, permite que ela aja de acordo com sua crença de que a informação deve ser irrelevante para os outros.

Do ponto de vista jurisprudencial, a construção majoritária da autodeterminação informativa enquanto direito no STF ocorre de forma similar à posição do tribunal alemão. Os dois tribunais, exercendo função de corte constitucional, entenderam o direito à autodeterminação informativa como consequência do princípio da dignidade da pessoa humana e dos direitos daí extraídos. Esses direitos formam o direito geral de personalidade, na perspectiva alemã, e o direito à inviolabilidade da intimidade e da vida privada, no contexto brasileiro. Com base nesses aspectos teóricos, o direito à autodeterminação informativa “se desvia de seu conteúdo material e desloca sua base para um poder de decisão formal e instrumentos procedimentais”¹⁵⁸.

¹⁵⁶ RODOTÀ, Stefano. **A vida na sociedade da vigilância**. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

¹⁵⁷ QUELLE, Claudia. Not just user control in the General Data Protection Regulation. On the problems with choice and paternalism, and on the point of data protection, Karlstad: Springer, 2017. In: LEHMANN, A.; *et al.* (orgs.). **Privacy and Identity Management - Facing up to Next Steps**. Karlstad: Springer, 2017.

¹⁵⁸ MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 239.

Porém, a transferência ampla para o titular do dever de controlar seus dados pessoais também é foco de críticas. Na forma como traduzida atualmente, a autodeterminação tem como consequência a imposição de um ônus para o titular exercer seus direitos de forma ampla, provocando os agentes de tratamento e o Judiciário, por exemplo. Além disso, as assimetrias econômicas e de informação no momento do consentimento, entendido como principal ferramenta para garantir a capacidade do indivíduo em autodeterminar-se, “puseram desafios concretos à proteção de dados concebida como uma espécie de autogestão”¹⁵⁹.

Diversos desafios surgem na tentativa de se concretizar a autodeterminação informativa, seja em vista da forma de decisão humana ou automatizada e nos riscos vislumbrados diante do uso de novas tecnologias. Esses desafios ocorrem pela complexidade da cadeia de responsáveis pelo tratamento de dados, pela quantidade massiva de informações pessoais tratadas para acesso a bens e serviços no mundo digital, pelo cruzamento de dados, e pela relevância dos dados inferidos. É nesse cenário que as vulnerabilidades do titular e as assimetrias de informação e de poder existentes “expõem a insuficiência da proteção de dados entendida como o direito de os indivíduos decidirem em princípio por si próprios quando e dentro de que limites seus dados podem ser utilizados”¹⁶⁰.

A autodeterminação informativa, como concebida nos moldes tradicionais do titular controlar individualmente qual terceiro e de que forma esse trata seus dados, encontra fronteiras em um cenário de assimetria entre os agentes de tratamento e os titulares de dados. Esse modelo é extraído da decisão alemã de 1983. Ao mesmo tempo, a autodeterminação inserida no âmbito de aplicação de um direito geral de personalidade alemão ganha novas interpretações e mecanismos de execução, em vista do seu caráter de adaptabilidade e flexibilidade. Por isso, faz-se necessária uma releitura do conceito para que ele fundamente o estabelecimento de uma estrutura mais complexa de controle. Essa estrutura está abarcada pela moldura de proteção de dados ao conceber que o titular de dados, junto a outros agentes, também exerce sua capacidade de controlar seus dados quando estes são tratados, em uma análise contextual, para uma finalidade previsível e de acordo com suas legítimas

¹⁵⁹ ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 181.

¹⁶⁰ ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. RB-11.3.

expectativas¹⁶¹. Nesse sentido, é possível construir o seguinte diagrama com os principais conceitos relacionados à autodeterminação:

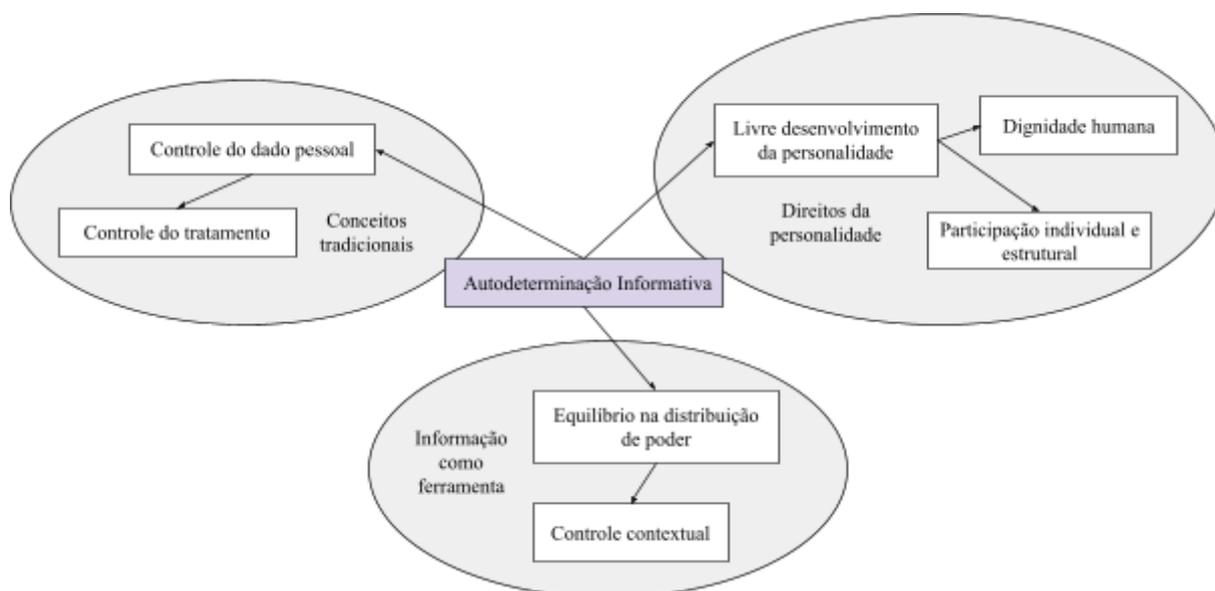


Figura 6 - Diagrama de conceitos relacionados à autodeterminação informativa

Tendo em vista a centralidade do conceito de autodeterminação informativa, diversos institutos jurídicos foram criados para a manutenção do controle do titular sobre seus próprios dados pessoais. Nesse sentido, há um regime jurídico de proteção de dados com princípios e direitos comuns em diversos ordenamentos que desenvolveram regulamentações sobre o tema. Esse regime inclui a aprovação dos *Standards* Internacionais sobre Proteção de Dados Pessoais, em 2009, na 31ª Conferência Internacional de Autoridades de Proteção de Dados. Colin Bennett reconhece esse movimento como fenômeno de convergência em que diversas jurisdições aprovaram legislações semelhantes em termos de conteúdo de forma a refletir um consenso e um padrão de regras sobre a forma de se proteger os dados pessoais durante a década de 1970¹⁶². Em regra, a convergência é explícita no estabelecimento de princípios e mecanismos para garantia da liberdade de controle ao titular sobre os dados pessoais¹⁶³.

Diante dessa concordância entre as regulamentações, Laura Schertel identifica que as normas europeias determinam, de maneira relativamente uniforme: (i) uma lei geral que se aplicaria a diversos contextos e com largo âmbito de aplicação; (ii) uma autoridade administrativa que seria encarregada de fiscalizar a aplicação da lei; (iii) um conceito amplo

¹⁶¹ BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 265 (item 5.4.2.5)

¹⁶² BENNETT, Colin. **Regulating privacy: data protection and public policy in Europe and the United States**. New York: Cornell University, 1992.

¹⁶³ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 6 e 45.

sobre dados pessoais e formas de tratamento; (iv) hipóteses de tratamento de dados, inclusive o consentimento; (v) princípios de proteção de dados, e, por fim; (vi) direitos subjetivos do titular¹⁶⁴. O modelo brasileiro está no âmbito de influência das normas europeias, em vista das similaridades em regular a proteção de dados. Nesse sentido, o impacto da autodeterminação é diretamente percebido nas determinações sobre os princípios da matéria e os direitos do titular previstos nessas normas, inclusive na LGPD, já que são instrumentos com função de possibilitar o controle do titular acerca de seus dados¹⁶⁵.

4. AS IMPLICAÇÕES DA AUTODETERMINAÇÃO INFORMATIVA COMO FUNDAMENTO DA LGPD

A estrutura da LGPD é baseada no modelo europeu, isso implica em uma importação dos padrões regulatórios de lá para o contexto brasileiro. São conhecidos pela doutrina dois modelos de regulação da proteção de dados: o modelo de proteção *ex ante*, encabeçado pela UE, e o *ex post*, dos Estados Unidos da América. O primeiro modelo é abrangente e regula a proteção de dados por uma lei geral, aplicável em diferentes contextos econômicos e sociais, de forma a ser possível responsabilizar o agente de tratamento por uma série de práticas para proteger o sujeito antes mesmo de um direito ser violado. Essa forma de regulação indica o tema como âmbito de incidência de políticas públicas, composto por direitos subjetivos aos titulares, “instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação”, as autoridades de proteção de dados nacionais¹⁶⁶.

Já o modelo *ex post* está associado a uma proteção contratual, em que os agentes de tratamento possuem maior liberdade para determinar a forma com que trataram dados pessoais, sem haver uma regulação geral, mas apenas setorial. Assim, esses agentes se vinculam apenas ao que foi explicitado em contrato, normalmente nas políticas de privacidade. A violação de direito surge da quebra desse contrato e, como consequência, não há uma autoridade de proteção que atua preventivamente, mas apenas um *enforcement* repressivo¹⁶⁷.

¹⁶⁴ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 47.

¹⁶⁵ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 46.

¹⁶⁶ MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado) - Faculdade de Direito da Universidade de Brasília, 2008, p. 134. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso: 10 nov. 2022.

¹⁶⁷ TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. In: ONODERA,

Enquanto fundamento da matéria, a autodeterminação informativa pode ser percebida como um fio condutor que direciona a interpretação a ser dada aos elementos descritos no tema de proteção de dados e na lei em questão. A título de exemplo, previsões como o direito de informação ao titular sobre os dados tratados visam facilitar o exercício de sua capacidade em controlar e determinar como um terceiro irá processar essa informação. Nesse sentido, este item se debruçará sobre os influxos da autodeterminação na conformação dos princípios e dos direitos dos titulares por serem dois elementos centrais na garantia do devido tratamento de dados pessoais, para que se possa projetar, a partir disso, um direito à explicação.

Como visto anteriormente (tópico 2), as decisões automatizadas baseadas em dados pessoais estão sendo utilizadas em diversos contextos e intensidades, de forma a impactar sobremaneira as escolhas e os comportamentos desses titulares. As aplicações de IA são utilizadas para automatizar, aprimorar e personalizar decisões a fim de reforçar uma lógica específica de conhecimento, antecipar fenômenos, avaliar a relevância de fatos personalizadas, entre outros¹⁶⁸. Diante desses tratamentos de dados e seus efeitos, a LGPD estabeleceu um direito do titular conhecer os critérios e procedimentos utilizados para o resultado da decisão automatizada, entendimento que também é impactado pelo fio condutor da autodeterminação. A partir das informações sobre a decisão, o desequilíbrio na relação de poder entre o controlador e o titular é relativamente minimizado e este passa a poder exercer minimamente um controle sobre o tratamento de seus dados pessoais, bem como os efeitos desse para seus interesses e direitos.

4.1. Princípios da LGPD relacionados à concretização da autodeterminação informativa

Um dos reflexos do movimento de convergência na regulação de proteção de dados pessoais a nível internacional, inclusive com o conceito de autodeterminação informativa, foi a elaboração dos princípios da matéria. Esses princípios têm como objetivo justamente direcionar o tratamento de dados pessoais e permitir que o titular possa exercer seu poder de autodeterminação. De forma direta, “[e]sses princípios têm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder ao indivíduo para que esse possa controlar o fluxo de seus dados”¹⁶⁹.

Marcus Vinicius (coord.); DE FILIPPO, Thiago Baldani (coord.). **Brasil e EUA: Temas de direito comparado**. São Paulo: Escola Paulista da Magistratura, 2017, p. 194.

¹⁶⁸ GILLESPIE, Tarleton. The Relevance of Algorithms. In: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo; FOOT, Kirsten. **Media Technologies**. Cambridge: MIT Press, 2013, p. 3.

¹⁶⁹ MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado) - Faculdade de Direito da Universidade de Brasília, 2008, p. 56. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso: 10 nov. 2022.

Um primeiro quadro comum de princípios sobre o tema ficou conhecido como *Fair Information Practice Principles* (FIPP) a partir da publicação do relatório *Records, Computers and the Rights of Citizens* do Departamento de Saúde, Educação e Bem-Estar dos EUA, em 1973. Esse relatório enunciava cinco princípios que deveriam ser observados no tratamento de dados: (i) não deve existir nenhum banco de dados pessoais cuja existência seja secreta; (ii) deve haver um meio para o indivíduo conhecer quais dados a seu respeito estão armazenados e de que forma eles são usados; (iii) deve existir um meio pelo qual o titular possa impedir que um dado obtido para uma finalidade seja utilizado para outros fins, sem o seu consentimento; (iv) deve existir um meio pelo qual o indivíduo possa corrigir ou emendar uma informação pessoal armazenada a seu respeito; (v) qualquer organização que crie, mantenha, use ou dissemine dados de pessoas identificadas deve garantir que a informação somente será usada da forma pretendida e deverá tomar as precauções razoáveis para prevenir o abuso do dado¹⁷⁰.

No mesmo período de tempo, ideias similares a esses princípios estavam presentes no relatório sobre risco do tratamento automatizado de dados realizado por organizações privadas elaborado pelo Comitê de Privacidade da Grã-Bretanha¹⁷¹ e na lei de proteção de dados do estado de Hesse, na Alemanha¹⁷². A partir de então, os princípios organizados no FIPP se consolidaram em regulações e documentos sobre proteção de dados como direcionamentos mínimos para garantia do titular, a exemplo das publicações sobre o tema feitas pela Organização para Cooperação e Desenvolvimento Econômico (OCDE) nos anos seguintes. Na década de 1980, a OCDE publicou os princípios base para a regulamentação do tema, reconhecendo o princípio da participação individual e a necessidade de informar o titular sobre a finalidade do tratamento, bem como sua extensão.

Os documentos publicados pela OCDE sobre o assunto, o *Privacy Guidelines*, de 1980 (que foram atualizados em 2013), e o *Declaration on Transborder Data Flows*, de 1985, influenciaram o desenvolvimento da matéria por meio do estabelecimento de padrões normativos aplicáveis internacionalmente sobre as práticas de proteção de dados pessoais¹⁷³.

¹⁷⁰ ESTADOS UNIDOS DA AMÉRICA. **Records, Computers and the Rights of Citizens**. Department of Health, Education and Welfare, 1973, p. 41. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 10 nov. 2022.

¹⁷¹ PARLIAMENT. Privacy: Younger Committee's Report. HL Deb 06 June 1973 vol 343 cc104-78. Disponível em: <https://api.parliament.uk/historic-hansard/lords/1973/jun/06/privacy-younger-committees-report>. Acesso em: 12 dez. 2022.

¹⁷² MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 70

¹⁷³ OCDE. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. 2013. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.h>

Essas ideias, inicialmente discutidas no FIPP, também foram replicadas na LGPD e resultaram em alguns dos princípios da lei. A tabela a seguir apresenta os princípios da OCDE e associa-os aos princípios da LGPD.

Princípios da OCDE	Princípios da LGPD
Limitação da Coleta: deve haver limites à coleta de dados pessoais e quaisquer desses dados devem ser obtidos por meios lícitos e justos e, quando apropriado, com o conhecimento ou consentimento do sujeito dos dados.	Finalidade, necessidade e adequação (art. 6º, I, II, III), além da boa-fé (art. 6º, <i>caput</i>)
Qualidade dos Dados: os dados pessoais devem ser relevantes para os fins para os quais serão utilizados e, na medida do necessário para esses fins, devem ser precisos, completos e mantidos atualizados.	Qualidade de dados (art. 6º, V)
Especificação da Finalidade: as finalidades para as quais os dados pessoais são coletados devem ser especificadas o mais tardar no momento da coleta de dados e o uso subsequente limitado ao cumprimento dessas finalidades ou de outras que não sejam incompatíveis com essas finalidades e que sejam especificadas em cada ocasião de mudança de finalidade.	Finalidade (art. 6º, I), além da boa-fé (art. 6º, <i>caput</i>)
Limitação de Uso: os dados pessoais não devem ser divulgados, disponibilizados ou utilizados para outros fins que não aqueles especificados de acordo com a finalidade, exceto: a) com o consentimento do titular dos dados; ou b) pela autoridade da lei.	Finalidade, necessidade e adequação (art. 6º, I, II, III)
Salvaguardas de Segurança: os dados pessoais devem ser protegidos por salvaguardas de segurança razoáveis contra riscos como perda ou acesso não autorizado, destruição, uso, modificação ou divulgação de dados.	Segurança (art. 6º, VII)
Transparência: deve haver uma política geral de transparência sobre desenvolvimentos, práticas e políticas com respeito aos dados pessoais. Os meios devem estar prontamente disponíveis para estabelecer a existência e natureza dos dados pessoais, e as principais finalidades de seu uso, bem como a identidade e residência habitual do responsável pelo tratamento dos dados.	Livre acesso, transparência e finalidade (art. 6º, IV, VI, I)
Participação Individual: o titular deve ter o direito de: a) obter de um controlador de dados, ou de outra forma, a confirmação de que o controlador de dados tem ou não dados relativos a ele; b) ser comunicado sobre dados relativos a ele b.1) dentro de	Livre acesso, transparência e qualidade de dados (art. 6º, IV, VI, V)

[tm#:~:text=Personal%20data%20should%20be%20protected.modification%20or%20disclosure%20of%20data..](#)
Acesso em: 12 dez. 2022.

<p>um prazo razoável, b.2) a uma taxa, se houver, que não seja excessiva, b.3) de uma maneira razoável, b.4) e de uma forma que seja facilmente inteligível para ele; c) receber razões se um pedido feito nos termos das alíneas (a) e (b) for negado, e poder contestar tal negação; e d) contestar os dados relativos a ele e, se a contestação for bem sucedida para que os dados sejam apagados, retificados, completados ou emendados.</p>	
<p>Responsabilização: o controlador de dados deve ser responsável pelo cumprimento das medidas que dão efeito aos princípios acima expostos.</p>	<p>Responsabilização e prestação de contas (art. 6º, X)</p>

Figura 7 - Tabela associativa dos princípios de proteção de dados da OCDE e da LGPD

Esses princípios se comunicam com o fundamento da autodeterminação na medida em que buscam garantir ferramentas para que o titular possa controlar o tratamento de dados o qual está exposto e participar da decisão sobre como suas informações são utilizadas. O princípio da segurança, por exemplo, determina que os agentes de tratamento utilizem medidas técnicas e administrativas adequadas para evitar acessos não autorizados, destruição, difusão indevida de dados, entre outros. O princípio da qualidade dos dados visa garantir que o tratamento se baseie em dados “adequados, pertinentes e não excessivos em relação à finalidade declarada, além de serem objetivos, exatos e atualizados”¹⁷⁴. Com isso, incumbe ao agente de tratamento manter dados verídicos sobre o titular, o que pode ser realizado por meio dos direitos do titular, como o de acesso, retificação e cancelamento dos dados pessoais, que serão evidenciados no subtópico adiante (tópico 4.2). No próximo subtópico, serão analisadas de forma mais detida a influência da autodeterminação na delimitação dos princípios da LGPD que dialogam com um direito à explicação individualmente considerados.

4.1.1. Princípios da transparência e do livre acesso

Os princípios da transparência e do livre acesso garantem ao titular informações claras, precisas e facilmente acessíveis sobre a forma e a duração do tratamento de dados e os agentes de tratamento envolvidos, observados os segredos comercial e industrial (art. 6º, IV e VI). É nessa mesma linha que o Considerando 39 do RGPD descreve os efeitos do princípio da transparência. A lei impõe ao agente de tratamento obrigações de, a partir de uma postura ativa, informar de maneira geral o titular sobre o tratamento de dados, independente deste solicitar essas informações. Além da informação em si, cabe ao agente de tratamento

¹⁷⁴ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 72.

disponibilizar mecanismos efetivos para que essas informações possam ser solicitadas e acessadas fácil e gratuitamente¹⁷⁵. Nos casos específicos de tratamento de dados realizado pelo poder público, para além dos princípios da transparência e do livre acesso, há incidência do princípio da publicidade. Os órgãos e entidades públicas devem prestar “informações claras e atualizadas sobre a previsão legal, finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades”, nos termos do art. 23, I. A ANPD poderá dispor sobre as formas de publicidade das operações de tratamento, nos termos do art. 23, §1º, da LGPD. No entanto, é possível afirmar que a obrigação de transparência é agravada quando o agente de tratamento é uma organização pública. Com esses princípios, a lei garante o aspecto material e formal da transparência no tratamento de dados pessoais delimitada no direito de informação, desenvolvido no subtópico (tópico 4.2.1) a seguir.

A centralidade do princípio da transparência na proteção de dados tem como fundamento a ideia de que ser transparente e disponibilizar informação é uma das formas de se combater os abusos os quais podem surgir com o tratamento de dados¹⁷⁶. Por meio das informações fornecidas pelo próprio agente de tratamento, este presta contas sobre o processamento de dados que realiza e o titular passa a ser munido de armas para se autodeterminar e exercer seus direitos. Apesar disso, o princípio da transparência também tem como público alvo outros atores envolvidos na proteção de dados, como as entidades da sociedade civil que se ocupam do tema, a autoridade de proteção de dados e a sociedade no geral. Por vezes, o tratamento é feito de forma massiva e possui efeitos para além dos titulares de dados sujeitos ao processamento de informações pessoais.

A fim de se delimitar o escopo do princípio da transparência, o Grupo de Trabalho do Art. 29 destaca a influência desse princípio em três áreas: (i) o fornecimento de informações aos titulares relacionadas ao tratamento adequado de dados; (ii) a comunicação entre os controladores e os titulares em relação aos direitos dos últimos e a forma facilitada de exercício desses direitos; e (iii) a comunicação entre os controladores e os titulares sobre violação de dados (*data breach*)¹⁷⁷. Dessa forma, por meio do respeito ao princípio da transparência, busca-se gerar confiança nos processos que afetam as pessoas, capacitando-as a

¹⁷⁵ BRASIL. Autoridade Nacional de Proteção de dados. **Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público**. 2022, p. 15. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico_defesa_eleitoral.pdf. Acesso em: 12 dez. 2022.

¹⁷⁶ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 71.

¹⁷⁷ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Transparency under Regulation 2016/679**. 2016. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>. Acesso em: 13 dez. 2022, p. 4

compreender e, se necessário, a desafiar esses processos. No entanto, o art. 6º, IV, da LGPD, expressamente compatibiliza a transparência às fronteiras do segredo de negócio, de forma que à transparência ser mitigada quando as informações a serem divulgadas facilitarem a adoção de práticas abusivas do ponto de vista comercial e isso afetar negativamente os interesses econômicos dos agentes envolvidos¹⁷⁸. Essa tensão será analisada nos tópicos seguintes (tópico 5.3 e 6.2).

Como destacado pelo Grupo de Trabalho, os princípios em questão criam obrigações de informação do controlador para com o titular associadas ao direito de informação, detalhado no tópico a seguir (tópico 4.2). Esse dever de informar para ser transparente é centrado no titular, de forma que a capacidade de se compreender as informações é tão importante quanto o próprio conteúdo das informações passadas pelo controlador sobre o tratamento dos dados. É a partir dessa informação clara, precisa e acessível que o titular será empoderado para exercer controle sobre seus dados pessoais, por exemplo, exercendo seus direitos e fornecendo ou retirando o consentimento informado.

Nesse sentido, o nível e a forma de transparência devem se adequar às circunstâncias do tratamento, inclusive se o titular faz parte de um grupo o qual merece proteção específica por lei, como as crianças. Isso quer dizer que o contexto e as vulnerabilidades dos titulares de dados devem ser levadas em conta pelo controlador em sua avaliação de como assegurar sua conformidade com suas obrigações de transparência¹⁷⁹. A transparência e o livre acesso são tensionados em um contexto de sistemas de IA opacos, como o *deep learning*, em que há pouca informação sobre seu funcionamento, inclusive para seus desenvolvedores.

Diante desses pressupostos, o princípio da transparência assume outros contornos quando aplicado às decisões automatizadas, que serão detalhados nos tópicos seguintes (tópico 5 e 6). A autoridade norueguesa entende que, para além das informações gerais na garantia do princípio da transparência, os titulares devem ser informados (i) de que os seus dados pessoais estão sendo coletados para uso em um sistema de tomada de decisão automatizada; (ii) da lógica subjacente do modelo, se as árvores de decisão são usadas e como os dados devem ser ponderados e correlacionados; (iii) dos impactos esperados no processo automatizado para o titular¹⁸⁰.

¹⁷⁸ FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais Fundamentos da LGPD**. 1. ed. Rio de Janeiro: Forense, 2022, p. 92.

¹⁷⁹ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Transparency under Regulation 2016/679**. 2016. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>. Acesso em: 13 dez. 2022, p. 11.

¹⁸⁰ DINAMARCA. Datatilsynet. **Artificial intelligence and privacy**. 2018. Disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Acesso em: 06 fev. 2023, p. 21

4.1.2. Princípios da finalidade, necessidade e adequação

Já os princípios da finalidade, necessidade e adequação figuram como uma tríade essencial para um tratamento de dados em acordo com a LGPD. Esse entendimento é consequência do impacto mútuo desses princípios na delimitação das práticas adequadas ou não à matéria de proteção de dados. O princípio da finalidade determina que o tratamento de dados deve estar associado a uma finalidade (i) legítima, que é “compatível com o ordenamento jurídico, além de amparada em uma base legal [...]”; (ii) específica, de maneira que a partir da finalidade seja possível delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais;” (iii) explícita; e (iv) informada, que seja disponibilizada de maneira clara e precisa, em linguagem simples, de fácil acesso e compreensão ao titular dos dados¹⁸¹.

Apenas nos casos em que o princípio da finalidade for devidamente atendido, enquanto princípio norteador do tema, o tratamento pode seguir para análise de sua conformidade com a lei, a qual deve passar pelo crivo dos outros princípios. A centralidade dessa tríade de princípios é destacada pelo STF na decisão das ADIs 6387, 6389, 6390 e 6393. O Ministro Luiz Fux entende que “[o] tratamento e compartilhamento de informações devem respeitar direitos e garantias individuais, sendo precedidos de uma adequada especificação das finalidades e medidas de segurança”¹⁸².

A finalidade é um princípio especialmente desafiador, já que avalia, por meio da motivação do agente em manter aquele tratamento, a adequação da prática. Se a justificativa a qual impulsiona o tratamento não for válida de acordo com os parâmetros supracitados, ele não deve prosperar. Ainda assim, se a finalidade for válida, mas o objeto do tratamento for excessivo, para além do essencial para se atingir a finalidade almejada, o tratamento viola o princípio da necessidade. Além disso, se a finalidade for válida e os dados imprescindíveis para alcançá-la, mas o tratamento não for compatível com a finalidade informada ao titular, o princípio da adequação é infringido.

¹⁸¹ BRASIL. Autoridade Nacional de Proteção de dados. **Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público**. 2022, p. 13. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico_defeso_eleitoral.pdf. Acesso em: 12 dez. 2022.

¹⁸²BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022, p. 66.

A aplicação dessa tríade de princípios é ainda mais complexa em um cenário de *big data* e coleta irrestrita de dados, já que os princípios impossibilitam o tratamento e o armazenamento de dados pessoais para fins indeterminados ou indetermináveis¹⁸³. Os princípios da LGPD vinculam o uso daquelas informações a um motivo compatível ao da coleta¹⁸⁴. A prática de mineração de dados coloca em risco o cumprimento desses princípios na medida em que a finalidade da mineração pode não ter sido apresentada ao titular. O tratamento de dados “insignificantes” pode revelar informações as quais o titular tinha expectativa de sigilo¹⁸⁵. A tentativa de extrair novas informações a partir dos dados informados pode ter como base dados excessivos coletados em desacordo com a necessidade concreta. O fenômeno do *big data* desafia a concretização desses princípios por aumentar significativamente a escala na coleta de dados, tratamento e capacidade de armazenamento, permitindo o estabelecimento de perfis a partir dos dados pessoais, levando em conta, ainda, o volume de dados tratados, bem como a variedade de fontes desses dados¹⁸⁶.

Para além disso, a conformidade de um tratamento com o princípio da finalidade é condicionada “à comunicação preventiva ao interessado sobre como serão usadas as informações coletadas; e para algumas categorias de dados especialmente sensíveis estabelece que a única finalidade admissível é o interesse da pessoa considerada”¹⁸⁷. Esse cenário de ampla disposição de informações pessoais agrava a aplicação dos princípios de transparência, finalidade, adequação e necessidade. Cabe ao controlador considerar o contexto da coleta dos

¹⁸³ MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005, p. 240. Disponível em: <https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50-anos-de-jurisprudencia-do-tribunal-constitucional-federal-alemao.pdf>. Acesso em: 11 nov 2022.

¹⁸⁴ DONEDA, Danilo; VIOLA, Mario. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. **Revista Brasileira de Risco e Seguro**, Rio de Janeiro, v. 5, n. 10, p. 85-102, out. 2009/mar. 2010, p. 98. Disponível em: <https://www.rbrs.com.br/arquivos/RBRS10-4%20Danilo%20Doneda.pdf>. Acesso em: 11 nov 2022. BRASIL. Autoridade Nacional de Proteção de dados. **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico_defeso_eleitoral.pdf. Acesso em: 07 mar. 2023, p. 13.

¹⁸⁵ MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado) - Faculdade de Direito da Universidade de Brasília, 2008, p. 104. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso: 10 nov. 2022.

¹⁸⁶ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 03/2013 on purpose limitation**. 2013, p. 55. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 13 dez. 2022.

¹⁸⁷ RODOTÁ, Stefano. **A vida na sociedade da vigilância**. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 87

dados, a finalidade concreta, as expectativas razoáveis dos titulares, a natureza dos dados pessoais e o impacto do tratamento sobre as pessoas¹⁸⁸.

Esse conjunto de princípios auxilia o titular a participar do tratamento de dados na medida em que fortalece o vínculo permanente entre o titular e o dado pessoal, expressão direta da personalidade humana¹⁸⁹. Mesmo quando conhecidos e tratados por terceiros, o uso de dados que tornam uma pessoa identificável pode refletir diretamente no titular. Assim, para que este possa exercer controle sobre seus dados, há de se garantir um tratamento de dados necessário e adequado para se atingir uma finalidade concreta, compatível e proporcional àquela do momento da coleta.

No contexto de decisões automatizadas, que são consequência de um contexto de *big data*, esses princípios encontram barreiras, por exemplo, na definição de quais são as finalidades e quais dados são necessários em um tratamento para treinamento de um algoritmo. A motivação pode inclusive mudar com o aprendizado e desenvolvimento da máquina¹⁹⁰. Esses princípios impõe, justamente, obrigações para o desenvolvedor dos sistemas considerar maneiras de atingir o objetivo da decisão automatizada de uma forma menos intrusiva para os titulares de dados, seja no volume de dados tratados, seja na sua natureza. Esses princípios auxiliam o agente de tratamento a minimizar o risco de dados pessoais irrelevantes serem utilizados para o algoritmo encontrar correlações que, em vez de significativas, são coincidências e nenhum peso deve ser atribuído a elas¹⁹¹. Assim, os sistemas de IA devem ser impactados pelos comandos de finalidade, adequação e necessidade do tratamento desde a sua concepção para que promovam controle de dados pelos titulares e estejam em acordo com o disposto na lei.

¹⁸⁸ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 03/2013 on purpose limitation**. 2013, p. 56. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 13 dez. 2022.

¹⁸⁹ DONEDA, Danilo; VIOLA, Mario. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. **Revista Brasileira de Risco e Seguro**, Rio de Janeiro, v. 5, n. 10, p. 85-102, out. 2009/mar. 2010, p. 98. Disponível em: <https://www.rbrs.com.br/arquivos/RBRS10-4%20Danilo%20Doneda.pdf>. Acesso em: 11 nov 2022.

¹⁹⁰ DINAMARCA. Datatilsynet. **Artificial intelligence and privacy**. 2018. Disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Acesso em: 06 fev. 2023, p. 18.

¹⁹¹ DATATILSYNET. **Artificial intelligence and privacy**. 2018. Disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Acesso em: 06 fev. 2023, p. 19.

4.1.3. Princípios da não discriminação, prevenção, responsabilização e prestação de contas

Também é possível interpretar o princípio da não discriminação por meio da autodeterminação informativa, já que o tratamento de dados para fins discriminatórios ilícitos ou abusivos necessariamente vai de encontro ao controle que o titular teria sobre seus dados pessoais ou qualquer forma de participação no processamento desses dados. Esse tipo de tratamento está em desacordo com os interesses do titular. Porém, a questão que suscita maior debate é a caracterização da ilicitude ou abusividade do tratamento discriminatório, isso porque esse tipo de tratamento viola o princípio em questão apenas quando a discriminação é ilícita ou abusiva, isto é, não é adequada, justa e pertinente para a finalidade pretendida¹⁹².

O princípio da não discriminação é violado quando o tratamento de dados pessoais (i) permite uma precificação diferenciada do mesmo produto a consumidores que estão em locais diferentes¹⁹³; (ii) prejudica candidatas mulheres no recrutamento de novos empregados pela condição do gênero¹⁹⁴; (iii) alega identificar traços faciais de terroristas por meio de características faciais¹⁹⁵, ou (iv) impede que mulheres trans e mulheres cis negras acessem aplicativo de relacionamento¹⁹⁶. Todo esse cenário de discriminação ilegal é intensificado com o desenvolvimento do *big data* e do uso de IA para tomada de decisões, já que, para além de outras questões, há pouca visibilidade dos fatores levados em consideração para se chegar a um resultado discriminatório e esse resultado é aplicado em massa aos titulares discriminados.

No entanto, existe uma zona cinzenta de discriminações que não são *a priori* ilícitas ou abusivas. Para fornecer parâmetros de análise sobre situações concretas, Laura Schertel e Marcela Mattiuzzo sistematizaram quatro tipos principais de discriminação algorítmica: (i) discriminação por erro estatístico; (ii) discriminação por generalização; (iii) discriminação

¹⁹² FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais Fundamentos da LGPD**. 1. ed. Rio de Janeiro: Forense, 2022, p. 99.

¹⁹³ BRASIL. Ministério da Justiça e Segurança Pública. **Decolar.com é multada por prática de geo pricing e geo blocking**. 2018. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/collective-nitf-content-51>. Acesso em: 02 jan. 2022.

¹⁹⁴ DASTIN, Jeffrey. **Amazon scraps secret AI recruiting tool that showed bias against women**. 2018. Disponível em:

<https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>. Acesso em: 31 jan. 2023.

¹⁹⁵ MCFARLAND, Matt. **Terrorist or pedophile? This start-up says it can out secrets by analyzing faces**. 2016. Disponível em:

<https://www.washingtonpost.com/news/innovations/wp/2016/05/24/terrorist-or-pedophile-this-start-up-says-it-can-out-secrets-by-analyzing-faces/>. Acesso em: 14 dez. 2022.

¹⁹⁶ RITSCHER, Chelsea. **'Female only' app criticised as 'transphobic' and 'racist' after AI software denies some women**. 2022. Disponível em:

<https://www.independent.co.uk/life-style/female-only-app-giggle-transphobic-b2002235.html>. Acesso em: 14 dez. 2022. Outros casos como este podem ser consultados em SILVA, Tarcízio. **Linha do Tempo do Racismo Algorítmico. Blog do Tarcízio Silva**, 2022. Disponível em: <https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo>. Acesso em: 12 dez. 2022.

pelo uso de informações sensíveis; (iv) discriminação limitadora do exercício de direitos¹⁹⁷. O primeiro diz respeito a erros na coleta e contabilização de dados ou na concepção técnica do algoritmo, já o segundo está relacionado a erros na classificação de pessoas e de objetos desses sistemas, por uma generalização que não se aplica no caso específico de pessoa atípica para aquela avaliação estatística. A discriminação pelo uso de informações sensíveis acontece quando, para a classificação, são utilizados dados sensíveis, características endógenas, e informações de grupos historicamente discriminados.

Para diferenciação de características endógenas (internas) e exógenas (externas), Laura Schertel e Marcela Mattiuzzo se utilizam de dois exemplos para evidenciar que as características endógenas estão intrinsecamente relacionadas com o efeito que provocam e apenas reforçam o resultado obtido. Um exemplo de característica endógena seria a falta de oportunidades igualitárias entre homens e mulheres no mercado de trabalho,

é possível afirmar que as mulheres foram, historicamente, mais envolvidas na criação dos filhos e em tarefas domésticas do que os homens. Mas esse é um resultado do fato de que a elas foram dadas menos oportunidades profissionais [...] e não uma característica inerente do sexo feminino que torna as mulheres menos capacitadas ou menos interessadas em oportunidades profissionais. A consequência da discriminação, nesse caso, leva à confirmação da hipótese inicial, pois estamos analisando uma variável endógena. Diferentemente, tomando-se o mercado de seguro de automóveis como exemplo, é fácil observar que o seguro para motoristas jovens do sexo masculino é mais caro do que o seguro para motoristas jovens do sexo feminino. O gênero guarda forte correlação com a taxa de acidentes de trânsito e, assim, é frequentemente utilizado para precificação. Neste segundo cenário, porém, o gênero não é uma variável endógena, mas sim exógena, pois nada no fato de que os homens pagam mais por seguros leva esse grupo a efetivamente se envolver em mais acidentes¹⁹⁸.

Por fim, o último tipo ocorre nos casos em que o titular de direitos é discriminado justamente por exercer seus direitos. Foi para evitar esse tipo de discriminação que o art. 21, da LGPD, proibiu o uso de dados pessoais em prejuízo do titular quando forem referentes ao exercício regular de direitos.

Um exemplo seria o SCHUFA, um *bureaus* de crédito alemão, que estava reduzindo a pontuação de score de crédito daqueles consumidores os quais buscavam exercer direito de acesso sobre seus dados. Isso porque a empresa utilizava o pedido de acesso aos dados como parâmetro negativo para gerar-se o score de crédito. À época, havia-se percebido uma correlação estatística de que pessoas que consultando seu score tinham maiores chances de adimplir. Essa prática deu causa à alteração da antiga lei de proteção de dados para vedá-la¹⁹⁹. Outro exemplo seria o caso da realização de background check no recrutamento de

¹⁹⁷ MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **RDU**, Porto Alegre, Volume 16, n. 90, 2019, 39-64, nov-dez 2019, p. 52-53.

¹⁹⁸
¹⁹⁹ DONEDA, Danilo *et al.* Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018, p. 6.

funcionários para a separação entre aqueles candidatos que são autores de alguma reclamação trabalhista para concretização de seus direitos e aqueles que não litigam contra seus empregadores. Em regra, essa discriminação é feita por meio do tratamento dos dados pessoais do candidato a fim de seja possível classificá-lo e, com isso, permitir que ele avance ou não em um processo seletivo.

Com essa classificação, são evidenciadas as possíveis causas de uma discriminação algorítmica que afronta o princípio em questão e, com isso, é possível descrever de forma mais precisa as práticas de tratamento de dados que estão ou não em conformidade com a não discriminação. Essa questão causa impacto ainda mais concreto no contexto de disseminação de decisões automatizadas baseada em dados pessoais, tendo em vista que, em regra, o mapeamento das possíveis discriminações é realizado depois que os danos já estiverem sido causados na sociedade. A capacidade do titular se autodeterminar quando está exposto a tratamentos discriminatórios abusivos ou ilícitos é expressivamente reduzida. Isso porque falta a garantia de ferramentas de participação individual ou estrutural naquele processo, ou mesmo a informação pessoal pode ter sido utilizada como ferramenta da manutenção do desequilíbrio na distribuição de poder em prejuízo do titular.

Em atenção a essas possíveis formas de tratamentos de dados, os princípios da prevenção (art. 6º, VIII) e da prestação de contas (art. 6º, X) têm como objetivo justamente criar um contexto em que os agentes de tratamento, constantemente, adotam medidas para prevenir a ocorrência de danos em virtude da sua atividade. Por meio desse princípio, os agentes demonstram a implementação dessas e outras medidas para atestar a conformidade do tratamento com a lei. Esses princípios estão associados à ampliação de competências decisórias do controlador²⁰⁰, já que o tratamento de dados passou a não depender apenas do consentimento, que era entendida como a principal ferramenta garantida ao titular para que este pudesse se autodeterminar.

O princípio de prevenção cria aos agentes de tratamento, principalmente o controlador, o dever de adotar ferramentas que previnam a ocorrência de danos aos titulares por meio, também, da preservação dos direitos deles. Quando esse princípio é cumprido, garante-se o direito de proteção de dados não apenas daquele sujeito que pode ser afetado pelo tratamento em concreto, mas toda a gama de titulares que eventualmente estariam expostos a esse risco de dano. No mesmo sentido, a prestação de contas é princípio resultado de “um processo que reúne múltiplos atores que se alternam no polo ativo e passivo, inclusive eventualmente

²⁰⁰ BIONI, Bruno Ricardo. *Accountability na regulação de dados pessoais: virtudes e vicissitudes*. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, 2021, p. 112.

mobilizando a opinião pública e as esferas administrativas e não apenas judicial se não estão de acordo”²⁰¹. Isso quer dizer que, para a observância desses princípios, não é suficiente a adoção estanque ou momentânea de práticas de prevenção e conformidade, é necessário constante atualização e aprimoramento das atividades de tratamento.

É diante do ato de prestação de contas feito pelo agente de tratamento que se ganha espaço para controlar e participar do processamento de seus dados pessoais, já que se percebe a não suficiência do agente alegar estar de acordo com a lei, mas caber a ele mostrar aos interessados suas práticas adequadas e torná-las verificáveis²⁰². Nesse sentido, destaca-se que a noção de controle, tradicionalmente associada à autodeterminação informativa e à proteção de dados de uma forma geral, e a ideia de prestação de contas, não necessariamente indicam para garantia irrestrita e absoluta de que o titular irá controlar todo o processamento de dados pessoais na prática²⁰³. É evidente a tensão entre os princípios de proteção de dados, especialmente a transparência, a finalidade e a prestação de contas, e as fronteiras de uma autodeterminação informativa entendida enquanto meio de controle sobre o tratamento de dados. Novos sentidos permeiam, tanto esse fundamento da LGPD, quanto as formas de concretização dos princípios diante dos desafios concretos impostos pela tecnologia, especialmente pelos sistemas de decisão automatizada.

Para além da proteção à capacidade do titular se autodeterminar, Bruno Bioni indica para um conceito de codeliberação informacional. Para o autor, “[o] que está em jogo é como uma plêiade de atores irá mobilizar suas respectivas prerrogativas jurídicas para reduzir a assimetria de poder em jogo e, com isso, experimentar um processo de codeliberação e não de dominação informacional”²⁰⁴. A partir deste conceito e dos influxos na busca de um sentido para a autodeterminação informativa na proteção de dados, nota-se que, cada vez mais, há uma preocupação com o âmbito coletivo da proteção. A matéria não se limita ao direito individual de controlar seus dados enquanto titular, mas busca o reequilíbrio de poder entre os atores envolvidos no processamento de dados. Estes atores podem incluir o titular, a sociedade, a autoridade de fiscalização, e o responsável por coletar, compartilhar, combinar, e

²⁰¹ BIONI, Bruno Ricardo. *Accountability na regulação de dados pessoais: virtudes e vicissitudes*. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, 2021, p. 242.

²⁰² UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 3/2010 on the principle of accountability**. 2010, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Acesso em: 12 dez. 2022.

²⁰³ LAZARO, Christophe; LE MÉTAYER, Daniel. **Control over personal data: true remedy or fairy tale?** SCRIPTed, vol. 12, issue 1, 2015. item 4.3. Disponível em: <https://script-ed.org/article/control-over-personal-data-true-remedy-or-fairy-tale/>. Acesso em 11 nov. 2022.

²⁰⁴ BIONI, Bruno Ricardo. *Accountability na regulação de dados pessoais: virtudes e vicissitudes*. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, 2021, p. 242.

inferir informações pessoais para atender os mais diversos interesses das organizações privadas ou mesmo do Estado.

4.2. Direito dos titulares

Uma das convergências do modelo regulatório da proteção de dados é o estabelecimento de direitos subjetivos, os quais podem ser exercidos pelos titulares de dados para que estes possam controlar o fluxo de suas informações pessoais em face dos responsáveis pelo tratamento²⁰⁵. O objetivo do estabelecimento de um rol de direitos está diretamente associado ao conceito de autodeterminação informativa, já que foi pensado como um mecanismo para efetivar o controle sobre dados pessoais. Nessa perspectiva, o Capítulo III da LGPD especifica os direitos garantidos ao titular de dados, que poderão ser exercidos a qualquer momento (art. 18, *caput*) e de forma gratuita (art. 18, §5º). Apesar da concentração neste capítulo, outras partes da lei também trazem direitos aos titulares de forma esparsa, como é o caso do direito à informação previsto no art. 9º, da lei. É possível notar o pressuposto da autodeterminação na efetivação desses direitos, como será explicitado a seguir.

Direito dos titulares previstos no art. 18, LGPD.	Conexão do direito em questão com a autodeterminação informativa.
Confirmação da existência do tratamento.	A partir da confirmação da existência do tratamento de dados, o titular poderá exercer controle sobre a atividade. Sem o direito de saber dessa prática, todos os outros direitos restariam prejudicados.
Acesso aos dados.	<p>Por meio do acesso aos dados pessoais, o titular passa a conhecer quais dados estão sendo tratados pelo controlador no momento do requerimento.</p> <p>No cenário atual, não há maiores direcionamentos sobre o escopo do direito de acesso aos dados, que serão determinados pela ANPD. Com isso, ainda há insegurança sobre a extensão do direito de acesso, formas de execução e limitações a esse</p>

²⁰⁵ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 65.

	<p>direito. Para Laura Schertel, esse direito “compreende o conhecimento sobre os dados armazenados, incluindo informações acerca da sua origem; sobre os organismos receptores das informações transmitidas ou a sua categoria; e sobre o objetivo do armazenamento”²⁰⁶.</p>
<p>Correção de dados incompletos, inexatos ou desatualizados.</p>	<p>Esse direito está associado ao princípio de qualidade dos dados, em que, por meio da alteração dos dados pessoais, é permitido que o titular controle quais informações serão processadas.</p>
<p>Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.</p>	<p>Diante de um descumprimento da lei, o titular poderá requerer a imposição de barreiras ao tratamento por meio do bloqueio ou eliminação dos dados, ou mesmo desvinculação desses com um pessoa identificada ou identificável.</p>
<p>Portabilidade dos dados, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.</p>	<p>Para que o titular exerça com autonomia sua capacidade de controle sobre os dados, a lei garante a ele o direito de transferir seus próprios dados para diferentes organizações.</p>
<p>Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses em que o agente de tratamento conserva dados para finalidades especificadas no art. 16, da LGPD.</p>	<p>Mesmo quando o tratamento de dados for lícito, o titular poderá controlá-lo solicitando que sejam eliminados retirando seu consentimento.</p>
<p>Informação das entidades públicas e privadas com as quais o controlador compartilhou seus dados</p>	<p>O titular conhecerá com quais organizações seus dados pessoais foram compartilhados, bem como a finalidade desse compartilhamento.</p>
<p>Informação sobre a possibilidade e as consequências de não fornecer consentimento</p>	<p>Para que o consentimento seja livre, informado e inequívoco, a lei estabelece o direito do titular de saber as repercussões do seu não consentimento quando esse é solicitado e, assim, de decidir de forma livre sobre o tratamento.</p>

²⁰⁶ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 66.

Revogação do consentimento.	Assim como o titular pode consentir com o tratamento de seus dados, também cabe a ele a qualquer momento não mais consentir com a prática, de forma a centralizar essa decisão na pessoa do titular.
Petição contra o controlador perante a autoridade nacional ou os organismos de defesa do consumidor.	Uma das facetas de controle do tratamento dos dados é a possibilidade do titular reclamar seus direitos e interesses para autoridades públicas.
Oposição ao tratamento que descumpra a LGPD, quando a hipótese legal não é consentimento.	Para além do bloqueio, eliminação e anonimização de dados, é possível que o titular se oponha ao tratamento de dados em desconformidade com a lei e isso sirva de barreira para a continuidade da prática.

Figura 8 - Tabela sobre a conexão dos direitos previstos no art. 18 da LGPD com a autodeterminação informativa

Esses direitos gerais estão sistematizados no art. 18 da LGPD, responsável pela compilação dos direitos subjetivos do titular, mas que não se limitam a apenas estes²⁰⁷. A lei, em todo seu texto, estabelece outros direitos decorrentes dos princípios de proteção de dados ou mesmo de seus enunciados normativos. A título de exemplo, tem-se o direito de livre desenvolvimento da personalidade (art. 1º) e de exigir o cumprimento de todas as obrigações previstas na lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular, mesmo quando o consentimento não for exigido (art. 6º, X, e art. 7º, §6º). Ainda assim, a lei garante direitos específicos ao titular quando o tratamento em questão ocorrer no âmbito de decisões automatizadas, que serão destacados a seguir. Ainda, a lei prevê que os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo (art. 21) e que o titular pode defender seus direitos em juízo, por meio de tutela individual ou coletiva (art. 22).

4.2.1. Direito de informação e de acesso aos dados

Apesar do fundamento da autodeterminação estar presente nos demais direitos dos titulares previstos na LGPD, a ideia de criar mecanismos de controle sobre dados pessoais no âmbito de decisões automatizadas está mais diretamente presente no direito de acesso e de informação. A lei entende ser a informação um dos mecanismos de “dar armas” ao titular para

²⁰⁷ FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais Fundamentos da LGPD**. 1. ed. Rio de Janeiro: Forense, 2022, p. 305.

que ele possa, de forma autônoma, proteger sua personalidade²⁰⁸. O direito geral de informação também decorre dos princípios do livre acesso e da transparência, já que, por meio da disponibilidade de informações ao titular, este passa a ter acesso facilitado à forma de tratamento de dados. Além disso, os demais princípios, como finalidade, necessidade, não discriminação e prestação de contas, são garantidos a partir de informações fornecidas ao titular para que, por meio delas, ele possa se perceber possíveis violações da lei.

De forma mais detida, o art. 9º da lei determina que o titular tem direito de ser informado sobre (i) a finalidade específica do tratamento; (ii) a forma e duração do tratamento; (iii) a identificação e o contato do controlador; (iv) o uso compartilhado de dados e a finalidade desse uso; (v) além das responsabilidades dos agentes envolvidos no tratamento de dados; e (vi) dos direitos dos titulares previstos na LGPD.

No entanto, ainda não há direcionamentos específicos sobre a execução e os limites desse direito de informação. Não estão definidas respostas a provocações como: qual a extensão do direito à informação ao titular? O que o controlador não está obrigado a informar? O controlador deve indicar a hipótese legal que ele se baseia para fundamentar cada fluxo de dados? É necessário informar o nome dos agentes de tratamentos que fazem uso compartilhado de dados ou apenas a indicação do setor daquele agente é suficiente? A indicação de qual função o agente de tratamento exerce na relação é adequada para informar sobre a responsabilidade de cada um? Qual o prazo para atender esse e outros direitos dos titulares?

Diante da centralidade dos direitos dos titulares para a proteção de dados, a ANPD incluiu em sua agenda regulatória para 2023 e 2024 a elaboração de uma iniciativa sobre o tema. Direitos dos titulares de dados pessoais estava descrito como tema a ser trabalhado pela ANPD desde a agenda Regulatória para o biênio 2021 e 2022 e, como não foi alcançado, manteve-se para a próxima agenda regulatória, que foi publicada como anexo da Portaria ANPD nº 35, de 4 de novembro de 2022²⁰⁹.

Para compreender o efeito concreto para o titular de um direito à informação, é possível perceber que a redação do art. 9º guarda semelhança com o disposto no art. 13 do RGPD, em vista da seguinte tabela de comparação:

²⁰⁸ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 66.

²⁰⁹ BRASIL. Diário Oficial. **Portaria ANPD nº 35, de 4 de novembro de 2022**. 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885>. Acesso em: 12 dez. 2022

Direito de informação na LGPD é traduzido no direito de ser informado sobre	Direito de informação no RGPD é traduzido no direito de ser informado sobre	Comentários
A finalidade do tratamento (art. 9º, I)	<p>As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento (art. 13 (1)(c))</p> <p>Os interesses legítimos do responsável pelo tratamento ou de terceiro, caso seja a base legal aplicada ao tratamento (art. 13 (1)(d))</p>	<p>Nos dois regimes, o titular deve ser informado sobre a finalidade do tratamento, o que reforça a relevância do princípio da finalidade.</p> <p>Porém, o RGPD prevê explicitamente a obrigação do controlador informar ao titular a base legal para o tratamento de dados. A LGPD é silente.</p>
A forma e duração do tratamento, observados os segredos comercial e industrial (art. 9º, II)	Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo (art. 13 (2)(a))	O RGPD não apresenta um dever de informação sobre a forma do tratamento, apenas sobre o período de tempo. No entanto, ainda não há maior detalhamento sobre os limites desse direito no caso brasileiro.
A identificação e o contato do controlador (art. 9º, III e IV)	A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante (art. 13 (1)(a))	Os dois regimes possuem previsões semelhantes.
N/A	Os contactos do encarregado da proteção de dados, se for caso disso (art. 13 (1)(b))	Na LGPD, o dever de informar o contato do encarregado não está compilado no art. 9º, mas no art. 41, §1º. Os efeitos das previsões são semelhantes.
O uso compartilhado de dados pelo controlador e a finalidade (art. 9º, V)	Os destinatários ou categorias de destinatários dos dados pessoais, se houver (art. 13 (1)(e))	O RGPD determina que o titular deve ser informado sobre (i) o destinatário do dado ou sua categoria; (ii) a

	<p>Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados (art. 13 (2)(e))</p> <p>O fato de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e as salvaguardas adotadas (art. 13 (1)(f))</p>	<p>transferência internacional e (iii) a obrigatoriedade do compartilhamento para atendimento de uma obrigação legal ou contratual.</p> <p>Já a LGPD não é específica sobre a necessidade de informar com quem os dados estão sendo compartilhados, mas apenas se há uso compartilhado, o que inclui casos de transferência internacional. Por outro lado, o controlador deve informar a finalidade do compartilhamento.</p>
<p>Responsabilidades dos agentes que realizarão o tratamento (art. 9º, VI)</p>	<p>N/A</p>	<p>Para o RGPD, o direito de ser informado sobre as responsabilidades dos agentes envolvidos não é consequência do direito de informação. Ao mesmo tempo, ainda não é uníssono a forma de execução desse requisito no contexto brasileiro. Não se sabe o escopo deste direito, diante do aspecto contratual em fixar essas responsabilidades. Não há clareza sobre se o controlador deve indicar de que forma é responsável pelo tratamento de dados e, se aplicável, como essa responsabilidade é compartilhada com outros agentes.</p>

Direitos do titular (art. 9º, VII)	A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de retirar o consentimento ou se opor ao tratamento, bem como do direito à portabilidade dos dados e de apresentar reclamação à autoridade (art. 13 (2)(b)(c)(d))	O conteúdo das previsões é semelhante. O RGPD é específico sobre os direitos que devem ser informados, mas que estão abarcados pela redação da LGPD.
N/A	A existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados (art. 13 (2)(f))	O direito de ser informado sobre a existência de decisões automatizadas não é especificamente previsto na LGPD, porém, como será visto a seguir, é um pressuposto para a execução do direito à revisão e à explicação previstos no art. 20, da LGPD.

Figura 9 - Tabela comparativa das consequências de um direito de informação

Diante da similaridade das ramificações de um direito à informação, o regulamento produzido pela União Europeia pode ser interessante para a formulação da ANPD sobre os direitos do titular. No contexto do Considerando 61 do RGPD, a informação deve ser garantida ao titular no momento da coleta do dado. Porém, não há obrigação de informar o titular em casos de tratamento de dados para fins estatísticos, de arquivo de interesse público, investigação científica ou histórica, observado o número de titulares de dados afetados, a antiguidade dos dados e as outras salvaguardas adotadas, em acordo com o Considerando 62. O RGPD também enuncia direitos específicos para situações em que os dados pessoais não são coletados junto ao titular, já que não há uma relação direta entre o titular e o agente de tratamento e, com isso, o sujeito pode não saber sobre o tratamento de dados feito por terceiros.

Porém, a LGPD não possui a mesma ressalva e trata de forma homogênea esses cenários. Para os casos em que os dados pessoais não foram obtidos diretamente pelo titular dos dados, o RGPD estabelece que o titular deve receber informações dentro de um período de tempo razoável, mas no máximo após um mês do recebimento dos dados por este terceiro agente de tratamento. Em regra, o controlador tem que fornecer as mesmas informações específicas como se os dados pessoais tivessem sido obtidos diretamente do titular. O controlador tem a obrigação de informar de quais fontes os dados pessoais foram originados e se eles estavam disponíveis ao público. Esse direito é especialmente relevante em um cenário de intenso fluxo de dados pessoais e constante compartilhamento de informações entre agentes de tratamento.

O direito de acesso é um direito específico de informar o titular, já que permite que ele acesse quais dados pessoais individualmente considerados o agente de tratamento está utilizando (art. 18, II). A LGPD destaca que o acesso de dados pessoais deve ser atendido imediatamente após requisição do titular, em formato simplificado, ou após 15 dias, para indicar a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial (art. 19). A partir do acesso aos dados tratados, seja por decisão automatizada ou não, o titular passa a ter direito de conhecer quais dados pessoais seu o agente de tratamento conhece e que, possivelmente, foram utilizados como *input* daquele sistema.

Na prática, esse direito à informação tem sido traduzido na publicação de políticas de privacidade por parte dos controladores de dados. Diversas empresas, autoridades e órgãos públicos, entidades da sociedade civil e demais organizações disponibilizam em seus websites informações relacionadas ao tratamento de dados que o titular está sujeito para que se alcance esse nível de informação especificado pela legislação. Garantir acesso facilitado a esse conteúdo está em acordo com essas regulamentações e é um elemento positivo no estabelecimento de confiança na relação entre o titular e o agente de tratamento²¹⁰. No entanto, o mero fornecimento de informações aos titulares é um exercício formalista que alcança resultados não significativos para a proteção de dados, o objetivo desse direito é informar pessoas e, com isso, aprimorar as decisões que tomam²¹¹.

²¹⁰ REINO UNIDO. Information Commissioner's Office. **Guide to the General Data Protection Regulation**. 2022. Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>. Acesso em: 07 dez. 2022, p. 164

²¹¹ SOLOVE, Daniel. The Limitations of Privacy Rights. **GW Law Faculty Publications and Other Works**, 2022, p. 19.

Em relação ao direito de informação aplicado às decisões automatizadas, o art. 9º, II, determina que o titular deve ser informado sobre a forma do tratamento de dados. Apesar do caráter indeterminado do termo, é possível depreender que, como consequência, a política de privacidade deve indicar se aquele agente realiza tratamento de dados por meio de sistemas de tomada de decisão automatizada. Isso porque saber da forma do tratamento permite que o titular e os interessados entendam como os dados pessoais são utilizados, inclusive quanto à maneira de tratamento que ocorre por meio do uso de sistemas automatizados.

Ao mesmo tempo, essa informação deve ser concisa, transparente, acessível e de fácil entendimento, a fim de cumprir o objetivo de manter o titular consciente sobre o ciclo de vida que os seus dados estão sujeitos naquela organização. Diante disso, outras ferramentas podem ser interessantes para que o titular receba adequadamente a informação, a exemplo do uso de ícones, de avisos *just-in-time*. Esse conteúdo se refere a informações de privacidade relevantes, focadas e entregues no momento em que o agente coleta informações sobre as pessoas, ou de painéis de controle, em que é apresentada ao titular uma ferramenta de gerenciamento de preferências²¹². Tanto o conteúdo da informação quanto a forma que ela é passada importam para a garantia do direito à informação.

4.2.2. Direito de revisão

Para além dos direitos gerais e tendo em vista as peculiaridades das decisões automatizadas, é garantido ao titular o direito de solicitar a revisão sempre que a decisão (i) for unicamente automatizada; (ii) tiver como base dados pessoais; e (iii) afetar os interesses do titular, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20). As delimitações conceituais de uma decisão tomada unicamente com base no tratamento automatizado de dados pessoais e que afeta os interesses do titular estão explícitas no segundo tópico (item 2.2) desta pesquisa.

Esse direito do titular solicitar que a decisão automatizada seja reanalisada pelo agente competente funciona como um meio de contestação em que a pessoa afetada requer a revisão naquela escolha por não concordar com o resultado final²¹³. Em vista do desequilíbrio informacional das partes envolvidas, a lei garante ao agente mais “fraco”, ou seja, aquele

²¹² REINO UNIDO. Information Commissioner’s Office. **Guide to the General Data Protection Regulation**. 2022. Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>. Acesso em: 07 dez. 2022, p. 166.

²¹³ SARDINHA, Adrine Nascimento Celestino. **Direito à informação e à revisão de decisões informatizadas: uma análise da LGPD**. Poro Alegre, v. 6, n. 2, p. 257-286, mai. 2022, p. 272.

munido de menor quantidade e qualidade de informação sobre o mecanismo decisional automatizado, a possibilidade de solicitar a revisão da decisão que o desfavoreceu. Esse direito é bastante semelhante ao direito geral de oposição garantido a qualquer tratamento de dados em desconformidade com a lei. Por meio da revisão, o agente de tratamento pode reconsiderar o apontado pelo titular e tomar uma nova posição, a partir dos fundamentos apontados pelo titular.

Para que a revisão da decisão aconteça, devem ser garantidas ferramentas ao titular para que ele possua chances reais e justas de, a partir da sua impugnação, a decisão automatizada seja eventualmente modificada. É neste sentido que um direito à explicação surge como imprescindível, como será analisado a seguir (item 5). Todavia, a forma que garante o direito à revisão foi ponto de debate durante o processo de veto presidencial e apreciação pelo Congresso Nacional do PL de Conversão nº 7, de 2019, oriundo da MP nº 869, de 2018, que foi convertida na Lei nº 13.853/2019, a qual modificou a LGPD.

Os vetos à Lei nº 13.853/2019 foram apreciados e parcialmente aprovados pelo Congresso Nacional sob o número de Veto nº 24/2019. Nas razões presidenciais do veto, registra-se que “tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores”²¹⁴. O veto retirou a expressão “por pessoa natural” do *caput* do art. 20 e o §3º do mesmo artigo que, em sua forma originária, previa o direito de revisão feita por humanos. Por um lado, há quem entenda que “a presença da pessoa natural é a única garantia de que decisões totalmente automatizadas possam ser minimamente explicáveis”, de modo que o veto teria esvaziado o direito de revisão²¹⁵. Por outro lado, há quem defenda que a obrigatoriedade de participação humana no processo de revisão significaria um relevante dispêndio de recursos que não necessariamente garantiriam uma reanálise adequada e suficiente para atender a expectativa do titular, diante dos pedidos massivos de revisão.

O direito de revisão, da forma como previsto no art. 20, sem a obrigação de reanálise por pessoa natural, não impede que uma pessoa participe da revisão de uma decisão automatizada. Essa possibilidade abre espaço para implementação de diversos níveis de intervenção eficaz a ser realizado por uma pessoa natural ou mesmo por uma máquina,

²¹⁴ BRASIL. Congresso Nacional. **Estudo do Veto nº 24/2019**. 2019. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7977991&ts=1630423600906&disposition=inline>. Acesso em: 12 dez. 2022.

²¹⁵ FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais Fundamentos da LGPD**. 1. ed. Rio de Janeiro: Forense, 2022, p. 340.

quando suficiente para garantir esse direito de impugnar uma escolha automatizada. Ao mesmo tempo, considerar concretizada uma revisão no mesmo sistema que decidiu pode apenas reforçar as falhas e discriminações do sistema questionado²¹⁶. Nesse sentido, a principal questão a ser preservada pelo direito de revisão é a de permitir que, por meio da sua concretização efetiva, possa-se vislumbrar resultados diferentes dos apresentados pela decisão original²¹⁷.

No modelo europeu, a regra é que os titulares não sejam expostos a decisões tomadas exclusivamente com base no tratamento automatizado de dados, como destacado no segundo tópico desta pesquisa. Dessa forma, o controlador tem o dever de aplicar medidas adequadas para salvaguardar os direitos, liberdades e legítimos interesses do titular dos dados, especialmente o direito de obter intervenção humana, manifestar seu ponto de vista e contestar a decisão. O art. 22(3) do RGPD deixa explícito a possibilidade do titular solicitar intervenção humana no processo de tomada de decisão, mesmo antes de uma possível contestação. No caso de revisão da decisão, o guideline do WP 29 destaca que a intervenção humana é um elemento chave, isso quer dizer que a revisão deve ser realizada por alguém que tenha a autoridade e a capacidade adequadas para mudar a decisão. O revisor deve realizar uma avaliação completa de todos os dados relevantes, incluindo qualquer informação adicional fornecida pelo sujeito dos dados²¹⁸. Como resultado dessa impugnação, o regulamento garante ao titular o direito de solicitar a revisão dessa decisão, mesmo que não de forma explícita. Em comparação com a LGPD, o RGPD restringe a possibilidade de utilizar ferramentas automatizadas para tomar decisões, e, a partir disso, garante o direito de revisão de uma decisão contestada pelo titular de dados.

Como especificado anteriormente, o art. 22 do RGPD estabelece uma vedação geral ao uso de sistemas automatizados no processo de tomada de decisão, sendo possível apenas quando atendidas uma das três hipóteses legais: (i) consentimento do titular; (ii) o direito da União ou do Estado-Membro autorizar; e (iii) tratamento for necessário para execução de contrato. Criar uma barreira para uso desses sistemas pode não estar alinhado ao uso massivo dessas soluções, que já ocorre em diversos setores da sociedade, como indicado nesta

²¹⁶ O'NEIL, Cathy. **Weapons of math destruction - how big data increases and threatens democracy**. Nova York: Crown, 2016.

²¹⁷ SOUZA, Carlos Affonso; PERONE, Christian; MAGRANI, Eduardo. O direito à explicação: entre a experiência europeia e a sua positivação na LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 267.

²¹⁸ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 27. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

pesquisa (tópico 2.3). Essa determinação pode banalizar a ferramenta do consentimento, sobrecarregar demasiado o titular, e colocar sobre ele o ônus dos riscos do tratamento. Além disso, pode haver a fragmentação da regulação das decisões automatizadas, deixando que os estados-membros legislem sobre a matéria, ou mesmo pode alargar sobremaneira os tratamentos necessários para celebração ou a execução de um contrato. Dessa forma, a escolha do legislador brasileiro de não vetar o tratamento de dados em decisões automatizadas parece mais aderente à realidade, inclusive ao estabelecer salvaguardas para essa forma de tratamento.

Ainda, o controlador de dados tem o dever de fornecer, a depender de uma solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a tomada de decisão, observados os segredos comercial e industrial (art. 20, §1º). Esse dever do controlador se reverte em um direito para titular ter acesso a informações específicas quando estiver diante de uma decisão unicamente automatizada baseada em dados pessoais. Diante das novas fronteiras criadas por este direito, a próxima parte desta pesquisa se dedicará a entender um panorama dessas delimitações no Brasil, na União Europeia, Colômbia e Uruguai. Estes dois últimos membros da Rede Ibero-americana de proteção de dados, que é um fórum criado para intercâmbio de informações e experiências na regulação de proteção de dados²¹⁹.

4.3. Síntese preliminar dos princípios e direitos da LGPD na garantia de uma autodeterminação informativa

Em regra, os princípios de uma lei de proteção de dados pessoais são inspirados em documentos dos anos 1970 e 1980 reconhecidos internacionalmente por traçarem os primeiros entendimentos sobre o tema. Dois exemplos são (i) a limitação da coleta e uso dos dados necessários a uma finalidade específica e informada ao titular, ou ao menos dentro de sua expectativa; e (ii) a imposição de obrigações de informação e de acesso aos dados pessoais garantidas pelos responsáveis pelo tratamento. Esses princípios direcionaram o mapeamento de possíveis meios para se assegurar a proteção de dados, como a especificação de direitos dos titulares, a definição do escopo das informações que deveriam estar à disposição do titular e a delimitação de obrigações ativas para a preservação de direitos e prestação de contas da atividade executada.

²¹⁹ BRASIL. Autoridade Nacional de Proteção de dados. **ANPD torna-se membro da Rede Ibero-Americana de proteção de dados**. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-membro-da-rede-ibero-americana-de-protecao-de-dados>. Acesso em: 09 mar. 2023.

Os princípios da transparência e do livre acesso visam, por meio da informação fornecida pelo agente de tratamento, dar armas para o titular questionar o tratamento de dados e combater eventuais abusos que possam surgir com o seu processamento. Já a finalidade, necessidade e adequação são princípios reciprocamente impactos pela noção de que o tratamento deve ter como objeto dados mínimos e adequados para se alcançar uma finalidade legítima, específica, explícita, e informada. Todos esses elementos garantem o vínculo, diferente de controle, que não pode ser desfeito entre o titular e a sua informação pessoal. O princípio da não discriminação indica para necessidade de tratamento não ilícitos ou abusivos para os interesses do titular, que é um dos sujeitos da prestação de contas, princípio associado à obrigação do agente ser proativo em comunicar suas práticas para estar em conformidade com as normas de proteção de dados.

A razão de ser dos direitos previstos na LGPD é garantir a devida proteção de dados, ou seja, os direitos específicos funcionam para assegurar o direito guarda-chuva de proteção de dados, objeto da LGPD. Ao mesmo tempo, esses direitos são consequência do desenvolvimento do conceito de autodeterminação informativa que, por meio da efetividade dessas prerrogativas, os titulares passam a ter ferramentas concretas para exercer controle sobre o uso de suas informações pessoais. Esse controle ocorre seja por meio de requerimento feito diretamente aos agentes de tratamento, seja por meio de ações proativas desses agentes na proteção dos dados e interesses dos titulares. Alinhada a ideia de autodeterminação, o direito de informação ganha proeminência ao criar a obrigação do agente de tratamento munir a pessoa titular com conteúdo sobre o tratamento de dados, a partir disso ela passa a poder exercer os outros direitos, como o de correção ou oposição.

Todavia, o direito de informação possui limitações de efetividade e suas fronteiras de aplicação ainda não estão especificamente detalhadas no contexto da LGPD, de modo a se formar uma série de provocações ainda não fixadas pela lei ou mesmo pela autoridade de proteção de dados, responsável por interpretar a lei. Por ser um contexto mais maduro, a experiência europeia pode, preliminarmente, jogar luz a algumas dúvidas sobre a extensão do direito à informação, bem como quais informações devem ou não ser apresentadas ao titular e em quais momentos esse direito deve ser efetivado. Uma questão relevante é a forma de execução desse direito, que pode se valer de ferramentas como ícones, avisos *just-in-time*, ou de painéis de controle apresentados ao titular de dados.

Diante das peculiaridades enfrentadas pelo titular para observância de sua autodeterminação quando exposto a decisões automatizadas, a LGPD, assim como o RGPD, estabeleceu um direito de revisão aplicável a esses casos. O titular é competente para requerer

que o resultado de uma decisão automatizada seja reanalisado pelo agente de tratamento de dados. Como consequência, é permitido que o titular impugne uma decisão quando este não esteja de acordo com a posição automatizada final e peça uma revisão, que pode ser executada por uma máquina ou por um humano. De forma diversa, o RGPD e o guia elaborado pelo Grupo de Trabalho do Art. 29 indicam pelo direito de revisão feito por um humano quando o titular não estiver de acordo com uma decisão automatizada como forma de garantir participação humana no processo decisório. No entanto, apenas a obrigação de que um humano revise a decisão pode não significar a formulação de resultados diferentes da decisão original, ideal para se assegurar a capacidade do titular se autodeterminar.

De forma geral, o desenvolvimento da tecnologia, especialmente daquela que utiliza massivamente dados pessoais, impõe novos desafios à definição de práticas em conformidade com uma noção de autodeterminação informativa. Por meio da previsão dos princípios e dos direitos na LGPD, busca-se garantir participação do titular no processo de tratamento de dados, mas a delimitação individual desse sentido atribuído à autodeterminação e a execução prática indicam para uma possível insuficiência de tal. É nesse sentido que ganham espaço para reflexão as ideias que se ocupam de uma autodeterminação em âmbito coletivo e centrada no equilíbrio do poder gerado a partir do tratamento de informações pessoais. Ao mesmo tempo, a lei de proteção de dados avança na definição de direitos a titulares expostos a decisões automatizadas interpretados a partir de autodeterminação informativa, como o analisado no tópico seguinte.

5. DIREITO À EXPLICAÇÃO

Os debates iniciais sobre um direito à explicação guardam origem nos princípios de proteção de dados para um tratamento em acordo com a boa-fé e *fairness*, já enunciada no FIPP²²⁰. A ideia de transparência, evidenciada nos princípios da LGPD, também está associada ao próprio desenvolvimento da tecnologia, que passou a tomar decisões impactantes para a sociedade e, com isso, tornou-se necessário motivar essas decisões²²¹. A capacidade do titular autodeterminar-se, seja na acepção tradicional ou em suas decorrências, é determinada também pela explicação que este passa a conhecer quando é submetido à decisões automatizadas baseadas em dados pessoais em um contexto de *big data*. No entanto, desde as primeiras manifestações da academia sobre esse direito, houve discordâncias sobre sua

²²⁰ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 209.

²²¹ PASQUALE, Frank. **The Black Box Society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015, p. 8.

existência e escopo. Por isso, este tópico busca explicar o que seria um direito à explicação e seus principais efeitos para os titulares de dados e para os controladores, bem como a sua extensão, se é que ele existe, na UE, no Uruguai, na Colômbia e no Brasil.

5.1. Explicabilidade na proteção de dados

Com o início do desenvolvimento da tecnologia, pesquisadores norte-americanos e europeus debateram sobre a necessidade de maior transparência sobre os sistemas de decisão automatizada. Nesse contexto inicial, transparência significava que (i) o código fonte do algoritmo e o conjunto de dados deveriam ser submetidos a escrutínio público; ou (ii) deveriam ser elaboradas avaliações de impacto algorítmico diante de denúncias de terceiros ou de auditorias externas²²². Porém, já nesse momento, percebeu-se que esses mecanismos não seriam suficientes para garantir maior transparência para os titulares afetados. Isso porque determinado nível de transparência não seria útil para eles, podendo inclusive causar danos, por minimizar a visibilidade das informações relevantes e distrair os titulares sobre o que realmente importa²²³.

A revisitação normativa sobre a existência de um direito à explicação no âmbito da proteção de dados foi retomada com o debate sobre os efeitos do RGPD para as decisões automatizadas, especificamente nos artigos 13(2)(f), 14(2)(g) e 15(1)(h). Esses dispositivos determinam, dentro de um escopo amplo de direito à informação, o direito do titular acessar e receber informação relevante sobre a lógica da decisão automatizada, bem como os efeitos do tratamento para o titular dos dados. Antes mesmo da entrada em vigor do RGPD, Goodman e Flaxman reconheceram um direito à explicação baseado nos efeitos desses artigos do regulamento. Para eles, era possível a intervenção dos titulares no processo de tomada de decisão, impondo novos parâmetros no desenvolvimento de um algoritmo ou exigindo supervisão adicional²²⁴. Assim, uma explicação razoável forneceria, no mínimo, relatos de como os dados de entrada se relacionam com as previsões finais, indicando quais parâmetros são relevantes na tomada de decisão de forma transparente e acessível aos titulares²²⁵.

No entanto, esse reconhecimento logo foi rebatido por Wachter, Mittelstadt e Floridi, que entendem pela não correspondência entre um direito à explicação e as obrigações de

²²² KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 210.

²²³ ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New media and society**, v. 20, n. 3, p. 973-989, 2018, p. 984.

²²⁴ GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”. **AI MAGAZINE**, 2017, p. 56.

²²⁵ GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”. **AI MAGAZINE**, 2017, p. 55.

notificar e informar sobre a lógica da decisão, sendo estas apenas um desdobramento do direito de informação²²⁶. Quanto à obrigação de notificar, para Wachter, Mittelstadt e Floridi, um direito à explicação não poderia derivar de um direito de notificação, acesso, tendo em vista que este direito é apenas um contrapeso aos deveres de notificação dos controladores. Assim, ele não implica na criação de um novo direito, e foi criado especificamente para permitir que o titular esteja ciente do tratamento e possa verificar sua legalidade²²⁷.

A associação entre o direito à explicação e os princípios de proteção de dados, além dos direitos gerais da matéria, é relevante para a definição do que seria, isto é, da extensão ou escopo, esse direito. Em vista dessa relação de retroalimentação entre direitos e princípios, o direito à explicação seria uma ferramenta disponível para que o titular exerça seus outros direitos quando exposto a uma decisão automatizada. Ainda, o titular possa perceber a observância dos princípios no tratamento automatizado, principalmente da transparência e livre acesso, finalidade, necessidade e adequação, e não discriminação. A partir dessas informações sobre a decisão automatizada, o titular teria ferramentas concretas para se autodeterminar, isto é, participar do processo de tratamento de dados e exercer controle contextual sobre suas informações. Como consequência, haveria cenário de maior equilíbrio na distribuição do poder garantido em uma sociedade da informação.

Margot Kaminski entende existir uma relação evidente entre os direitos individuais de proteção de dados, como a contestação, correção e apagamento, e o tipo de transparência individualizada que a matéria requer²²⁸. Com isso, a autora evidencia que a substância de outros direitos subjacentes determina a extensão do princípio da transparência. Assim, se o titular tem um direito de correção, ele precisa ser capaz de ver erros possíveis em sistemas automatizados. Se o titular tem um direito de não discriminação, ele precisa ter as ferramentas para ver quais fatores são usados em uma decisão automatizada. Caso contrário, as assimetrias de informação tornam os direitos subjacentes efetivamente nulos²²⁹.

Para Wachter e outros, um direito à explicação teria dois significados diferentes: (i) um referente à funcionalidade do sistema, ou seja, a lógica, consequências previstas e funcionalidade geral de um sistema automatizado de tomada de decisão; e (ii) outro sobre as

²²⁶ WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017, p. 77.

²²⁷ WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017, p. 97.

²²⁸ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 213.

²²⁹ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 213.

decisões automatizadas específicas, que seriam as razões e as circunstâncias individuais de uma decisão específica, não geral. Ainda, essa explicação poderia ser dada (i) antes da tomada de decisão, que não estaria associada a explicações sobre uma decisão específica por suas características ainda não terem sido analisadas, ou (ii) após a decisão ser fixada, podendo abordar tanto a funcionalidade do sistema quanto a decisão específica²³⁰.

Nesse sentido, para que um direito à explicação específico passasse a existir, esses requisitos deveriam ser definidos, tendo em vista a fundamentalidade dessas condições para aplicação concreta do direito. Na lógica da explicação, os controladores deveriam apresentar evidências de decisões automatizadas relativas às características (*features*) levadas em consideração, ponderação do peso dessas características, árvore de decisão ou estrutura de classificação e lógica geral do sistema de tomada de decisão automatizada²³¹. Para os autores, a previsão de um direito à explicação possui implicação direta na concretização de outros direitos, como o direito de contestar a decisão, que não teria razão de ser se o titular não possuísse as ferramentas para entender como as decisões foram tomadas²³².

Usando a classificação de Wachter e outros sobre a funcionalidade do sistema e as decisões automatizadas específicas, as explicações da funcionalidade do sistema incluem, entre outros, a especificação de seus requisitos, as árvores de decisão, os modelos pré-definidos, os critérios e as estruturas de classificação. Já as explicações sobre as decisões específicas incluem informações sobre a ponderação de *features*, as regras de decisão específicas de cada caso, e dados sobre grupos de referência ou de perfil²³³. Porém, Selbst e Powles entendem não existir tal separação.

Para eles, as regras e a ponderação de *features* os quais constituem o sistema algorítmico decidem os casos de forma semelhante e consistente. Isso quer dizer que, segundo os autores, é difícil construir uma explicação relevante da funcionalidade do sistema a qual não oferece informações significativas sobre decisões específicas. Isso porque, por definição,

²³⁰ WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017, p. 78.

²³¹ WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017, p. 97.

²³² WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017, p. 97.

²³³ WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017, p. 78.

um titular precisaria de explicação suficiente para reivindicar seus direitos²³⁴. Assim, o que realmente importaria seriam os dados de entrada, tendo em vista a necessidade dos mesmo para determinar a decisão específica, mas uma vez que o modelo é construído e os dados de entrada são conhecidos, a lógica determina o resultado²³⁵.

Uma posição explícita nos quatro artigos de referência para descrição de um direito à explicação é a relevância desse direito para que o titular possa exercer seus direitos de proteção de dados, como oposição e contestação do tratamento, além da revisão da decisão²³⁶. Com isso, é possível concluir que esse direito está intrinsecamente associado aos princípios de proteção de dados, bem como demais direitos dos titulares. Sem um direito à explicação, o titular estaria de mãos atadas para exercer seus outros direitos e verificar se o tratamento de dados é devido. Por meio dele, o titular poderia verificar se está sujeito a uma decisão automatizada, qual a finalidade dela, quais dados foram levados em consideração, se são dados atualizados, se ele é discriminado abusiva ou ilegalmente, entre outros requisitos de conformidade com a matéria.

O direito à explicação está abarcado por todo o sistema de proteção de dados e se relaciona com ele. O fundamento da autodeterminação informativa é reafirmado em uma lógica de explicação, já que, sem ela, o titular passa a não ter ferramentas de controle sobre seus dados pessoais quando utilizados em decisões automatizadas, de forma a afetar seu livre desenvolvimento da personalidade. Entender a forma de regulação da matéria no RGPD é relevante para o estabelecimento de suas decorrências e influências, inclusive na LGPD. Nesse sentido, para se atingir esse direito à explicação, outras formas de transparência podem incidir em casos concretos. Muito se discute sobre o acesso ao algoritmo em seu formato de desenvolvimento, com expressões matemáticas e regras não acessíveis para pessoas leigas. Porém, diante de um direito à informação contextual, pode não ser útil que as pessoas tenham acesso a essas informações, mas pode ser útil para outros agentes²³⁷.

²³⁴ SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017, p. 240.

²³⁵ SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017, p. 239.

²³⁶ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 215. GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”. **AI MAGAZINE**, 2017, p. 55. WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017, p. 97. SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017, p. 242.

²³⁷ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 215.

Por isso, o direito à explicação, diante de um ecossistema de proteção de dados, garante que os titulares tenham acesso a uma forma de explicação, e especialistas e reguladores a outra²³⁸. Esta abordagem multifacetada da transparência não deve ser descartada, já que esse direito é mais profundo do que um simples sistema de respostas contrafactuais²³⁹ ou uma visão sistêmica e superficial. Nesse sentido, Kaminski entende que um direito à explicação está acoplado a outras medidas de transparência que vão no sentido de fornecer supervisão tanto de terceiros quanto de reguladores sobre a tomada de decisões algorítmicas²⁴⁰.

Portanto, o direito à explicação deve ser interpretado de forma funcional, flexível, e deve, no mínimo, permitir que o sujeito dos dados exerça seus direitos previstos na lei de proteção de dados e nas leis de direitos humanos²⁴¹. Isso não significa que esse direito crie a necessidade de uma explicação completa do funcionamento do sistema²⁴². Em resumo, o direito à explicação é um direito do titular ser informado, com conteúdo significativo, relevante, sobre a lógica adotada no processo de tomada de decisão. Isso é alcançado diante dos seguintes requisitos, que vão de uma explicação simples para uma explicação complexa:

²³⁸ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 217.

²³⁹ WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual explanations without opening the black box: automated decisions and the GDPR. **Harvard Journal of Law & Technology**, v. 31, n. 2, Spring, 2018, p. 41.

²⁴⁰ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 217.

²⁴¹ SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017, p. 242.

²⁴² SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017, p. 239.

Checklist do direito à explicação	
<input type="checkbox"/>	O interessado recebe informações de acordo com o risco do sistema para os direitos do titular, principalmente dos direitos de personalidade;
<input type="checkbox"/>	O interessado recebe informações de acordo com seu interesse e expectativa, se titular, auditor externo, auditor interno, autoridade de proteção de dados;
<input type="checkbox"/>	O titular sabe que está exposto a sistemas que tratam dados pessoais para decisões automatizadas;
<input type="checkbox"/>	O titular sabe os parâmetros de tratamento e sua ponderação baseado no modelo do sistema;
<input type="checkbox"/>	O titular sabe quais os dados pessoais são tratados pelo sistema e suas fontes;
<input type="checkbox"/>	O titular sabe qual a finalidade, a duração e quem é o controlador responsável pelo tratamento realizado pelo sistema;
<input type="checkbox"/>	O titular sabe o grau e o modo de contribuição do processamento automatizado para a decisão tomada;
<input type="checkbox"/>	O titular sabe o impacto e os efeitos da decisão tomada pelo sistema;
<input type="checkbox"/>	O titular sabe os parâmetros de tratamento e, quando apropriado, sua ponderação no caso concreto;
<input type="checkbox"/>	O titular sabe quais mudanças em seus dados de entrada (inputs) teriam feito com que a decisão automatizada fosse diferente;
<input type="checkbox"/>	O titular sabe como os inputs são transformados em outputs, informações que, por definição, podem não ser completas;
<input type="checkbox"/>	O titular sabe as intenções na criação do modelo, os parâmetros utilizados para treinar o sistema, e as características do sistema de IA utilizado;
<input type="checkbox"/>	O titular sabe as métricas de performance do sistema, em quais casos mais falha e a capacidade de previsão do sistema quando utilizado em dados diferentes dos de treinamento;
<input type="checkbox"/>	O titular sabe quais são as características dos indivíduos que receberam tratamento semelhante ao dele;
<input type="checkbox"/>	O titular sabe as propriedades não desejadas do sistema e como ele decide nessas situações.

Figura 10 - Checklist do direito à explicação²⁴³

A explicação pode variar de acordo com o contexto da aplicação do sistema de decisão automatizada, como quem são os titulares afetados, quais os riscos envolvidos, que tipo de serviço é ofertado, entre outros. Assim, informações mais básicas e menos complexas estão na caixa verdade da figura acima, e seus aprofundamentos estão nas caixas laranja e vermelha. Todo esse arcabouço de um direito à explicação está relacionado à possibilidade do interessado na decisão saber os motivos que levaram o sistema a decidir pelo resultado específico. Com isso, é possível que esse interessado analise os parâmetros da decisão, os

²⁴³ Esta checklist foi elaborada com base nos seguintes artigos: EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a “right to explanation” is probably not the remedy you are looking for. **Duke Law and Technology Review**, v. 16, n. 1, 2017, p. 58. EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”? **IEEE Security & Privacy**, v. 16, n. 3, 2018, p. 5. REINO UNIDO. Information Commissioner’s Office. **Explaining decisions made with IA**. 2022, p. 52. Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf>. Acesso em: 14 mar. 2023.

elementos levados em consideração, e encontre inconsistências e questionamentos tanto sobre a forma de decidir, quanto sobre o resultado final.

Essa inclinação de explicar escolhas guarda similaridade com o art. 93, IX, da Constituição Federal. Dentro de outro contexto do enfrentado nesta pesquisa, de um Estado Democrático de Direito, a Constituição determina a necessidade de fundamentação em todas as decisões do Poder Judiciário. Isso quer dizer que os juízes, enquanto legitimados pelo Estado, “devem expor as razões que os conduziram a eleger uma solução determinada em sua tarefa de dirimir conflitos”, cumprindo um dever fundamental de prestar contas quanto à coerência e equanimidade das decisões²⁴⁴. Esta pesquisa não afirma que o peso de uma decisão judicial é o mesmo de decisões automatizadas impactadas por um direito à explicação. Porém, essa previsão na Constituição indica para o interesse da sociedade brasileira, organizada em um Estado Democrático de Direito, em não estar sujeita a decisões arbitrárias, que não podem ser contestadas ou mesmo analisadas.

Sistemas de IA como ferramentas de explicação

É útil entender as características das justificações humanas para se ter visibilidade do que é necessário levar em consideração em uma explicação de decisão feita por algoritmo considerada juridicamente adequada. Para a execução de um direito à explicação, busca-se produzir fundamentações de decisões automatizadas compreensíveis e relevantes, assim como as explicações humanas adequadas. As explicações humanas, em regra, são: (i) contrastantes; (ii) seletivas; e (iii) contextuais²⁴⁵. Ou seja, para que uma explicação humana seja formada, (i) argumenta-se, respectivamente, por causas ou eventos que não ocorreram, a exemplo da negativa de crédito porque a pessoa não pagou a fatura do cartão de crédito; (ii) decide-se com base em informações relevantes e específicas, que ignoram leis gerais ou uma cadeia causal completa, as quais podem indicar para outros resultados; e (iii) utiliza-se de interações sociais para adaptar as explicações de acordo às crenças e capacidades de compreensão do destinatário, as quais podem, inclusive, ser complementadas a partir de novas perguntas²⁴⁶.

Essas características da explicação humana são levadas em conta também para elaboração de tecnologias explicáveis desde os seus desenvolvimentos, as chamadas “*Explainable AI*” (XAI). O objetivo das XAI é justamente produzir um sistema explicável

²⁴⁴ MENDES, Gilmar Ferreira; GONET BRANCO, Paulo Gustavo; **Curso de Direito Constitucional**. 14. ed. São Paulo: Saraiva Educação, 2019, p. 1077 a 1079.

²⁴⁵ MITTELSTADT, Brent; RUSSELL, Chris; WACHTER, Sandra. Explaining Explanations in AI. **FAT* '19: Conference on Fairness, Accountability, and Transparency**, January, 2019, Atlanta, Georgia, USA, p. 5.

²⁴⁶ MITTELSTADT, Brent; RUSSELL, Chris; WACHTER, Sandra. Explaining Explanations in AI. **FAT* '19: Conference on Fairness, Accountability, and Transparency**, January, 2019, Atlanta, Georgia, USA, p. 5 e 6.

para os padrões humanos, mesmo diante de suas complexidades técnicas, de forma que os sistemas IA funcionem como ferramentas de explicação por si próprios. Para tanto, além das explicações fornecidas pelos desenvolvedores, os sistemas de XAI permitem que os próprios sistemas de IA sejam capazes de elaborar diversos métodos de explicação, ou seja, se comportem como algoritmos geradores dessas explicações. Os métodos de explicação podem fornecer transparência sobre o sistema, que abarca uma compreensão técnica do funcionamento, de componentes individuais, sobre o algoritmo de treinamento, se aplicável, e sobre a forma e o motivo da decisão específica produzida pelo sistema²⁴⁷.

Esses algoritmos de explicação levam em consideração (i) a complexidade do algoritmo a ser explicado; (ii) a linguagem ou estrutura gerada pelo método diante dos limites de compreensão humana, que podem ser semelhantes a regras “se x, então y”, árvores de decisão, soma das ponderações dos *features*, ou mesmo a linguagem humana; e (iii) a nitidez do sistema, ou seja, o vínculo entre o método de explicação e o próprio sistema a ser explicado. Isso porque a transparência do sistema pode variar a depender do método, como no caso da baixa clareza de métodos que dependem apenas da manipulação de *inputs* e da observação de *outputs* por utilizar poucas informações para gerar explicações. Dessa forma, a explicação final pode ser resultado de associações entre os pesos das características (*features*) e o próprio modelo algorítmico para produzir justificativa compreensível a um humano²⁴⁸.

Com a aplicação de XAI, o direito à explicação passa ser concretizado com auxílio do próprio sistema de IA, que fornece informações sobre a forma de decisão automatizada. A adoção da própria tecnologia para gerar explicação sobre o seu funcionamento foi uma necessidade identificada diante do desenvolvimento de sistemas de aprendizagem de máquina e do impacto desses sistemas na vida cotidiana. A partir dessa necessidade, percebeu-se que técnicas de XAI são relevantes em casos de pouca confiabilidade nos sistemas de IA por falta de transparência ou quando busca-se tornar o modelo compreensível, inclusive usando explicações contratuais em sistemas que utilizam *deep learning*²⁴⁹. Assim, a explicabilidade

²⁴⁷ MITTELSTADT, Brent; RUSSELL, Chris; WACHTER, Sandra. Explaining Explanations in AI. **FAT* '19: Conference on Fairness, Accountability, and Transparency**, January, 2019, Atlanta, Georgia, USA, p. 2. RIBEIRO, Marco Tulio; SINGH, Sameer; GUESTRIN, Carlos. "Why Should I Trust You?": Explaining the Predictions of Any Classifier. **Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, ACM Press, 2016, p. 1135–1144, p. 1135.

²⁴⁸ MOLNAR, Christoph. **Interpretable Machine Learning: a guide for making black box models explainable**. 2. ed. 2022. Capítulo 3- *interpretability*. Disponível em: <https://christophm.github.io/interpretable-ml-book/>. Acesso em: 05 jan. 2023.

²⁴⁹ ARRIETA, Alejandro *et al.* Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. **Information Fusion**, Volume 58, 2020, Pages 82-115, ISSN 1566-2535, p. 101

do modelo depende da proteção dos dados, além da confidencialidade, imparcialidade e responsabilidade pensados no desenvolvimento do modelo²⁵⁰.

Explicabilidade no PL n° 2338/2023, que dispõe sobre regulação da IA

A necessidade de explicações sobre sistemas autônomos não está restrita ao debate de dados pessoais. O tema perpassa inclusive as discussões sobre uma possível regulação dos usos de IA em sentido amplo. Outro âmbito que é atravessado pela explicabilidade dos sistemas e o direito à explicação é a definição de estratégias nacionais para o desenvolvimento da IA. A Estratégia Brasileira de Inteligência Artificial, elaborada pelo Ministério da Ciência, Tecnologia e Inovações, apresenta a explicabilidade como elemento incentivador da rastreabilidade do processo decisório por meio do fornecimento de informações significativas que permitam interpretar o sistema²⁵¹. No Congresso Nacional, está em discussão o PL n° 2338/2023 e outros apensados, que dispõe sobre princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial, inclusive estabelecendo obrigações de explicabilidade no uso desses sistemas. Entre maio e abril de 2022, foram realizadas audiências públicas e seminários organizados pela comissão de juristas do Senado Federal²⁵², no âmbito do PL n° 20/2021, para discutir, entre outros temas, a explicabilidade dos sistemas de IA.

Nessa oportunidade de audiência pública, especialistas brasileiros destacaram a relevância de um direito à explicação que observe os limites de compreensão e conhecimento dos receptores dessa informação, seja o titular, público em geral, ou os profissionais da área²⁵³. A mera publicização do código-fonte do sistema poderia não atender às necessidades do titular e colocar os mecanismos de segurança do sistema em risco²⁵⁴. Segundo os participantes, o segredo de negócio pode ser um óbice à transparência, ao mesmo tempo a

²⁵⁰ ARRIETA, Alejandro *et al.* Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. **Information Fusion**, Volume 58, 2020, Pages 82-115, ISSN 1566-2535, p. 108.

²⁵¹ BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Estratégia Brasileira de Inteligência Artificial**. 2021, p. 19. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf. Acesso em: 12 jan. 2023.

²⁵² BRASIL. Senado Federal. **CJSUBIA**. [S.I.]. Disponível em: <https://legis.senado.leg.br/comissoes/comissao?codcol=2504>. Acesso em: 17 jan. 2023.

²⁵³ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado n° 4, de 2022, aprovado em 1° de dezembro de 2022. Brasília, 2022, p. 241.

²⁵⁴ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado n° 4, de 2022, aprovado em 1° de dezembro de 2022. Brasília, 2022, p. 109, 111 a 113.

falta de acesso à informação compromete a fiscalização e auditoria sobre os sistemas²⁵⁵. Porém, não houve consenso sobre a viabilidade de explicações das decisões tomadas por esses sistemas, diante de sua opacidade, acompanhada da necessidade de confiança nessa tecnologia por conhecer seu funcionamento e evitar violação de direitos²⁵⁶.

No seminário internacional, especialistas estrangeiros indicaram a explicabilidade como ferramenta para garantir que o sistema está observando os preceitos estabelecidos em lei, bem como supervisionar o seu funcionamento²⁵⁷. Ainda, a explicação e a transparência sobre o sistema devem permitir que “as pessoas sejam capazes de desafiar, contestar esses sistemas, de modo a vermos que há uma segurança robusta e crescente”²⁵⁸. Para tanto, elaboração de avaliações de impacto, registros do sistema, monitoramento de mercado e documentação técnica podem auxiliar no processo de uso das funcionalidades da IA²⁵⁹. Outra forma de criar medidas de explicação seria impedir que as plataformas se utilizassem de interfaces que enganam, manipulam, exerçam influência indevida ou incapacite o titular de escolher, em vista da assimetria de informações entre os agentes²⁶⁰.

Como consequência das contribuições orais, escritas e dos próprios estudos da comissão, foi elaborada uma minuta de substitutivo ao PL nº 21/2020, que foi apresentado como PL nº 2338/2023 pelo presidente do Senado em maio de 2023. Esse novo texto do PL estabelece, em seu art. 7º, um direito de as pessoas afetadas receberem informações claras e adequadas antes mesmo de utilizarem os sistemas de IA. Essas informações são sobre (i) caráter automatizado da interação e da decisão em processos ou produtos que afetem a pessoa;

²⁵⁵ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 111.

²⁵⁶ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 115.

²⁵⁷ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 190.

²⁵⁸ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 191.

²⁵⁹ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 191.

²⁶⁰ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 192.

(ii) descrição geral do sistema, tipos de decisões, recomendações ou previsões que se destina a fazer e consequências de sua utilização para a pessoa; (iii) identificação dos operadores do sistema de inteligência artificial e medidas de governança adotadas no desenvolvimento e emprego do sistema; (iv) papel do sistema de inteligência artificial e dos humanos envolvidos no processo de tomada de decisão, previsão ou recomendação; (v) categorias de dados pessoais utilizados no contexto do funcionamento do sistema de inteligência artificial; (vi) medidas de segurança, de não discriminação e de confiabilidade adotadas, incluindo acurácia, precisão e cobertura; e (vii) outras informações definidas em regulamento.

O art. 8º do PL estabelece que, após a decisão automatizada, cabe à pessoa afetada solicitar gratuita e facilitadamente explicação sobre uma decisão, previsão ou recomendação específicas, com informações a respeito dos critérios e dos procedimentos utilizados, e os principais fatores que afetam tal decisão. Essas informações incluem: (i) a racionalidade e a lógica do sistema, bem como o significado e as consequências previstas de tal decisão para a pessoa afetada; (ii) o grau e o nível de contribuição do sistema de inteligência artificial para a tomada de decisões; (iii) os dados processados e a sua fonte, bem como os critérios para a tomada de decisão e, quando apropriado, a sua ponderação, aplicados à situação da pessoa afetada; (iv) os mecanismos por meio dos quais a pessoa pode contestar a decisão; e (v) a possibilidade de solicitar intervenção humana, nos termos desta lei.

Nota-se que, apesar de não explicitamente, a minuta garante à pessoa afetada, para além apenas do titular de dados, direito à explicação geral, panorâmica, sobre o sistema de decisão, e específica, com as características levadas em consideração no caso concreto. Ainda, avança ao previsto na LGPD e determina a possibilidade de intervenção humana quando utilizados sistemas de IA. O PL enumera o rol de obrigações de informação que devem ser cumpridas pelo responsável pelo sistema antes e/ou depois da decisão automatizada, neste último, a depender do requerimento do interessado.

Explicabilidade e autodeterminação informativa

Apesar de inicialmente o direito à explicação decorrer do princípio da transparência²⁶¹, ele não se confunde com a simples obrigação de ser transparente sobre o processo de tomada de decisão automatizada. Esse direito se relaciona com diversos outros princípios de proteção de dados, como é o princípio da prevenção, responsabilização e prestação de contas. Esse complexo de elementos “colabora na construção de espaços de deliberação para discutir o que

²⁶¹ MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**, Artigo Estratégico, n. 39, 2018, p. 5.

seria ‘informação qualificada’ ou como mitigar problemas em decisões futuras [...] e possibilita endereçar questionamentos a respeito dos segredos comercial e industrial”²⁶².

Diante do exposto, o direito à explicação é uma das decorrências do fundamento da autodeterminação, conceito que passa por um processo de ressignificação. A perspectiva do titular ocupar o centro do tratamento de dados o coloca em evidência para participar e controlar o uso que é feito com seus dados e, com isso, diminuir a disparidade de informação e poder entre os atores envolvidos nesse processo. Um dos mecanismos para permitir essa minimização do desequilíbrio de poder é a explicação sobre o sistema automatizado que o titular é submetido para que, a partir de informações concedidas a ele, ele possa compreender, questionar, perceber incongruências e opor-se ao tratamento de dados.

É razoável perceber a necessidade de se utilizar sistemas de decisão explicáveis e, para tanto, esses sistemas devem ser capazes de responder perguntas comumente feitas a processos de decisões humanas. Assim, será possível notar se e onde as demandas de explicação devem ser diferentes entre os sistemas de IA e os humanos²⁶³. Essa equiparação entre perguntas feitas a humanos e máquinas é interessante para que se evite um cenário em que os sistemas autônomos tenham “passe livre” para decidir sem nenhum escrutínio, como aquele o qual os humanos passam, ou mesmo exigir tanto desses sistemas a ponto de dificultar a inovação e o desenvolvimento tecnológico²⁶⁴.

Após essa análise sobre um direito à explicação, é possível depreender cinco informações: (i) a autodeterminação informativa possui como um dos filtros o direito à explicação, de forma a reafirmar a centralidade do titular na proteção de dados e no livre desenvolvimento de sua personalidade; (ii) o direito à explicação não é igual à transparência, este conceito é um princípio amplo aplicável às normas de proteção de dados e que abarca, além da explicação de uma decisão automatizada, outros mecanismos; (iii) no âmbito da proteção de dados, o direito à explicação é um direito de informação específico aplicável às decisões automatizadas relevantes aos interesses dos titulares e baseadas em dados pessoais; (iv) ainda não há uma definição unânime sobre quais elementos compõem taxativamente um direito à explicação, mas, por meio dele, busca-se saber sobre a racionalidade de uma decisão

²⁶² BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana. MULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019, p. 218.

²⁶³ DOSHI-VELEZ, Finale *et al.* Accountability of AI Under the Law: The Role of Explanation. **arXiv:1711.01134**. 2019, p. 21 Disponível em: <https://doi.org/10.48550/arXiv.1711.01134>. Acesso em: 15 mar. 2023.

²⁶⁴ DOSHI-VELEZ, Finale *et al.* Accountability of AI Under the Law: The Role of Explanation. **arXiv:1711.01134**. 2019, p. 21 Disponível em: <https://doi.org/10.48550/arXiv.1711.01134>. Acesso em: 15 mar. 2023.

automatizada; (v) não foi definido o momento que esta explicação deve ser dada, uma corrente afirma pelo direito de solicitar explicações antes do tratamento de dados e outra corrente defende a concretização desse direito após a decisão ser feita, guardada a proporção da explicação a ser dada.

5.2. Um direito à explicação em decisões automatizadas baseadas em dados pessoais na União Europeia, Uruguai e Colômbia

Em vista do debate sobre a existência e a extensão de um direito à explicação enquanto um dos direitos determinados pela matéria de proteção de dados no Brasil, as experiências estrangeiras auxiliam na compreensão de um contorno sobre o tema. A prática de outros países dá concretude aos direitos de proteção de dados. Isso ocorre seja pelos textos normativos, orientações das autoridades de proteção de dados, ou seja pelo esforço doutrinário para compatibilizar as regras já estabelecidas com uma realidade decorrente do *big data* e da disseminação de sistemas de IA baseados em dados pessoais.

Como visto anteriormente, o debate sobre um direito à explicação intitulado dessa forma ganhou novo fôlego com a vigência do RGPD. O regulamento avançou no tema de decisões automatizadas regulado pela Diretiva 95/46/CE, revogada pelo regulamento. A discussão sobre um direito à explicação nas decisões automatizadas é anterior ao regulamento²⁶⁵. Desde 1978, o art. 3º da Lei de Informática e Liberdades francesa estabeleceu um direito da pessoa conhecer as informações e razões utilizadas nos tratamentos automatizados cujos resultados se opõem.

Com o RGPD, a UE encabeça os debates acadêmicos sobre se um direito à explicação está previsto na norma de proteção de dados e, se sim, de que forma esse direito poderia ser concretizado. A regulação europeia, seja pelo RGPD, seja pela Diretiva, possui capacidade de influenciar a agenda regulatória de outros países, bem como as práticas do mercado. Assim, as normas produzidas pela UE se tornam referência e fonte de interpretação para outros contextos. Esse fenômeno foi denominado *Brussels Effect* e descreve justamente o poder de influência regulatória da UE. A UE, sem recorrer a instituições internacionais ou buscar a cooperação de outros países, é capaz de promulgar regulamentos que se enraízam nos quadros

²⁶⁵ VERONESE, Alexandre. Capítulo 14. Os direitos de explicação e de oposição diante das decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. RB-14.3.

jurídicos de mercados desenvolvidos e em desenvolvimento, levando a centralização de aspectos importantes do comércio global nas mãos da UE²⁶⁶.

A partir do parâmetro construído na UE sobre direito à explicação das decisões automatizadas, é possível analisar a experiência de outras jurisdições próximas ao Brasil para a definição de um direito à explicação. Os exemplos do Uruguai e Colômbia são relevantes para essa análise em vista das diferenças e complementaridades das jurisdições na regulação dessa forma de tratamento de dados pessoais. Uruguai e Colômbia foram as jurisdições analisadas nesta pesquisa por terem proximidade com o Brasil, em um contexto de América Latina, e tratarem o tema de decisões automatizadas no âmbito da proteção de dados de forma diversa entre si e em relação ao Brasil. A análise sobre os cenários da União Europeia, Uruguai e Colômbia se limitou à redação da lei de proteção de dados local e posições doutrinárias a respeito de um direito à explicação, não se buscando analisar a incidência do texto legal no contexto cultural, econômico e jurídico dos países. O tema não é tratado de maneira simétrica, por isso essa análise evidencia diferentes formas de se garantir ferramentas de explicabilidade, seja por meio de informações ao titular ou de transparência no tratamento de dados pessoais.

5.2.1. UE: Regulamento (UE) 2016/276, de 2016

O RGPD regula a tomada de decisão automatizada baseada em dados pessoais por meio de quatro artigos específicos, além de todo arcabouço normativo do regulamento, seus princípios, direitos, bases legais e medidas de conformidade com a lei. Como descrito anteriormente, o RGPD prevê especificamente, nos artigos 13(2)(f), 14(2)(g) e 15(1)(h), o direito do titular receber, quando obtidos os dados, e acessar, a qualquer momento, informação relevante (útil, significativa) sobre a lógica da decisão automatizada, bem como a importância e os efeitos do tratamento para o titular dos dados. Como será evidenciado a seguir, ainda não há uma definição unânime e concreta do que seriam “informações relevantes sobre a lógica do sistema”. Apesar disso, existem desafios associados à própria definição de “informações relevantes sobre a lógica do sistema” em abstrato.

Uma pesquisa conduzida por Dexe *et al.* a respeito do direito à explicação a decisões automatizadas exercido por titulares em face de empresas de seguro indica que um desafio para empresas analisadas é a diferença de interpretação na própria exigência de informações significativas sobre decisões algorítmicas. Isso tanto em termos de como o parágrafo da lei é formulado (em qualquer idioma) quanto no fato de que as versões em diferentes idiomas

²⁶⁶ BRADFORD, Anu. The Brussels Effect. *Northwestern University Law Review*, v. 107, n. 1, 2012, p. 64

parecem apontar para diferentes interpretações. Isso cria incerteza no mercado e, para evitar esse cenário, esclarecimentos de tribunais ou legisladores são necessários²⁶⁷. O regulamento, no art. 22, também estabelece obrigações mínimas a serem observadas pelo controlador quando for possível sujeitar o titular a decisões automatizadas, já que a regra é a proibição do uso desses sistemas. Dentre essas obrigações, cabe ao responsável pelo tratamento aplicar medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, como, no mínimo, o direito de obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão automatizada, sempre que ela se basear no consentimento ou execução de contrato.

²⁶⁷ DEXE, Jacob *et al.* Explaining automated decision-making: a multinational study of the GDPR right to meaningful information. **Geneva Pap Risk Insur Issues Pract**, n. 47, 2022, p. 693.

Regulamento (UE) 2016/279, de 2016

Artigo 13

2. Para além das informações referidas no n.1, quando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:

f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22, n. 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Artigo 14

2. Para além das informações referidas no n.1, o responsável pelo tratamento fornece ao titular as seguintes informações, necessárias para garantir um tratamento equitativo e transparente:

g) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22, n. 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Artigo 15

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:

h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22, n. 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Artigo 22

3. Nos casos a que se referem o n. 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.

Figura 11 - Artigos relevantes para um direito à explicação na UE (tradução livre)

A partir dessas determinações, formou-se um debate, majoritariamente acadêmico, sobre se elas seriam suficientes para estabelecer um direito à explicação sobre as decisões automatizadas na UE²⁶⁸ levado a cabo por Goodman e Flaxman²⁶⁹, e Wachter, Mittelstadt e

²⁶⁸ CONSELHO DA EUROPA. **128th Session of the Committee of Ministers**. 2018. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf. Acesso em: 09 jan. 2023.

²⁶⁹ GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”. **AI MAGAZINE**, 2017.

Floridi²⁷⁰. Apesar da discussão, o texto expresso do RGPD determina um direito de informação, nos art. 13(2)(f) e art. 14(2)(g), e um direito de acesso, no art. 15(1)(h), resultado das obrigações de transparência, que auxiliam o controlador a estar de acordo com as medidas adequadas para salvaguardar os direitos, liberdades e legítimos interesses do titular, como previsto no art. 22(3)²⁷¹. O *European Union Agency for Fundamental Rights*, quando apresenta os direitos dos titulares, relacionado o disposto no art. 13(2)(f) com um direito à explicação, mais especificamente a um *right to meaningful explanation*, reforçando a ideia de um direito à explicação no RGPD²⁷².

A respeito do direito de informação, o grupo de trabalho do Artigo 29 estabelece que as informações úteis relativas à lógica do sistema incluem os critérios utilizados para se chegar na decisão final e outras informações suficientemente abrangentes para que o titular entenda as razões da decisão. Dessa forma, a exemplo do *score* de crédito, caberia aos *bureaus* de crédito informarem as principais características consideradas para chegar à decisão, a fonte destas informações e o peso delas, o que inclui por exemplo: (i) informações fornecidas pelo sujeito dos dados no formulário de requerimento; (ii) informações sobre a conduta da conta anterior, incluindo qualquer pagamento em atraso; e (iii) informações oficiais de registros públicos, tais como informações de registros de fraude e registros de insolvência²⁷³. O titular deve ser informado sobre a importância e as consequências do tratamento a fim de conhecer como ele será afetado por aquela decisão por meio de exemplos.

Já o direito de acesso permite que o titular conheça uma decisão automatizada tomada e comunique-se sobre o tratamento de dados. Assim, o controlador deve fornecer ao titular dos dados informação geral que lhe seja útil para contestar a decisão, nomeadamente, sobre os fatores levados em conta para o processo de tomada de decisão, e sobre o respetivo peso a nível agregado. Para o grupo de trabalho, isso significa dizer que, pelo direito de acesso, não

²⁷⁰ WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017.

²⁷¹ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 24. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

²⁷² UNIÃO EUROPEIA. European Union Agency for Fundamental Rights. **Handbook on European data protection law**. Luxembourg: Publications Office of the European Union, 2018, p. 205.

²⁷³ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 26. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

existe um direito à explicação sobre uma decisão automatizada individualmente considerada, os titulares devem receber informações sobre as consequências do tratamento²⁷⁴.

Para grande parte da comunidade acadêmica, esses dois direitos seriam suficientes para se perceber um direito à explicação, já que permite, a partir dessas informações, que o titular exerça seus direitos²⁷⁵. No entanto, Wachter e outros acadêmicos entendem que não existe um direito à explicação no RGPD, já que o regulamento, em seu texto com força normativa, não o prevê de forma explícita. Haveria apenas um direito especial de informação quando tratamento importar em decisões automatizadas que seria mais fraco que um direito à explicação. Essa interpretação só é possível porque esses acadêmicos igualam o direito à explicação “como popularmente proposto” com o direito de explicações *ex post* de decisões específicas²⁷⁶, porém essa não é a única forma de se garantir um direito à explicação. Importa destacar que, segundo as diretrizes do grupo de trabalho, o titular tem direito de conhecer: (i) as categorias de dados usados na decisão automatizada²⁷⁷; (ii) a fonte dos dados²⁷⁸; (iii) os fatores levados em consideração para a decisão²⁷⁹; (iv) o “peso”, relevância, desses fatores para a decisão²⁸⁰; (v) os motivos²⁸¹; (vi) além da importância e consequência da decisão.

Além disso, o art. 22(3) do RGPD determina a necessidade do controlador adotar outras medidas para salvaguardar os titulares quando a decisão se basear no consentimento ou execução de contrato, mas não especifica quais medidas seriam essas, apenas que deveriam

²⁷⁴ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 17. Disponível em: <https://ec.europa.eu/newsroom/article29/redirect/document/49826>. Acesso em: 08 dez. 2022.

²⁷⁵ SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017, p. 242.

²⁷⁶ SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017, p. 238

²⁷⁷ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 17. Disponível em: <https://ec.europa.eu/newsroom/article29/redirect/document/49826>. Acesso em: 08 dez. 2022.

²⁷⁸ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 26. Disponível em: <https://ec.europa.eu/newsroom/article29/redirect/document/49826>. Acesso em: 08 dez. 2022.

²⁷⁹ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 27. Disponível em: <https://ec.europa.eu/newsroom/article29/redirect/document/49826>. Acesso em: 08 dez. 2022.

²⁸⁰ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 27. Disponível em: <https://ec.europa.eu/newsroom/article29/redirect/document/49826>. Acesso em: 08 dez. 2022.

²⁸¹ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 25. Disponível em: <https://ec.europa.eu/newsroom/article29/redirect/document/49826>. Acesso em: 08 dez. 2022.

incluir, no mínimo, uma forma de o titular obter intervenção humana, expressar seu ponto de vista e contestar a decisão. Para evidenciar de forma mais detalhada essas medidas, o grupo de trabalho destaca o Considerando 71 do RGPD, o qual descreve que, em qualquer caso, as garantias adequadas devem incluir também o direito de obter explicação sobre a decisão tomada após o resultado final e o direito de contestar a decisão²⁸². O controlador deve fornecer uma maneira simples para o titular dos dados exercer esses direitos, o que enfatiza a necessidade de transparência sobre o tratamento²⁸³. Isso porque o titular só poderá contestar uma decisão ou expressar a sua opinião se compreender plenamente como foi tomada e com que fundamento.

No sistema europeu, os considerandos são dispositivos sem força normativa, mas que conferem interpretações às previsões estabelecidas nas leis, de forma que os considerandos do RGPD funcionam como guias para as determinações mais objetivas descritas nos seus artigos. Nesse sentido, Kaminski entende que o Regulamento é “um regime de governança colaborativa, tendo em vista que o seu texto está repleto de normas amplas, que receberão substância específica ao longo do tempo por meio de diálogos contínuos entre reguladores e regulados, eventualmente respaldados por tribunais”²⁸⁴. Assim, a autora considera que quando os acadêmicos argumentam que o que está nos Considerandos é não a lei, eles não estão apenas insistindo em um tecnicismo, distinguindo entre instrumentos jurídicos mais rígidos e mais flexíveis, como também estão desconsiderando a natureza fundamentalmente colaborativa e evolutiva do RGPD e removendo importantes fontes de clareza para as empresas à medida que a lei se desenvolve.

As diretrizes do grupo de trabalho declaram que os indivíduos não precisam conhecer o código-fonte ou as explicações matemáticas complexas referente ao sistema de decisão²⁸⁵. Há uma preocupação maior com a transparência do sistema, seja informando o escopo da decisão automatizada, propósito comercial, seja apresentando as implicações legais ou

²⁸² UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 27. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

²⁸³ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 27. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

²⁸⁴ KAMINSKI, Margot E. The Right to Explanation, Explained. *Berkeley Technology Law Journal*, v. 34, n. 1, 2019, p. 195.

²⁸⁵ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 25. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

práticas do sistema, do que uma simples legitimidade do algoritmo²⁸⁶. Essa determinação é relevante para destacar que a forma de explicar as decisões importa, mais especificamente, o “quem” e o “porquê” da transparência determinada pelo RGPD determinam o “quê”, “quando” e “como” deve ser informado²⁸⁷. Não é adequado que os titulares recebam informações não relevantes ou úteis, sem que possam de fato compreender o conteúdo do que está sendo informado. Isso porque as disposições de transparência individual destinam-se a capacitar os indivíduos a invocar seus outros direitos previstos no RGPD, de acordo com Considerando 60.

Mais do que um direito à explicação, mas ainda relacionado a ele, o RGPD e as diretrizes do grupo de trabalho estabelecem outras medidas de transparência e, com base nisso, Kaminski destaca três medidas relevantes aplicáveis às decisões automatizadas²⁸⁸. Primeiro, pelo art. 58(1)(b)(e), as autoridades de proteção de dados têm competência para realizar auditorias e acessar todos os dados pessoais tratados pelo controlador ou operador de dados, de forma a estar munida de recursos significativos para obter acesso a informações sobre algoritmos. Em segundo lugar, com base no art. 35(3)(a), os controladores devem elaborar um relatório de impacto à proteção de dados em casos de decisões baseadas no tratamento automatizado de dados pessoais, mesmo que o processo não seja completamente automatizado. Por último, as diretrizes sugerem que os controladores realizem auditorias independentes e forneçam ao auditor todas as informações necessárias sobre como o algoritmo ou sistema de aprendizado de máquina funciona sempre que se utilizar de tomada de decisão baseada em perfis com um alto impacto sobre os indivíduos²⁸⁹.

5.2.2. Uruguai: Lei nº 18.331, de 2008

A proteção de dados pessoais no Uruguai é principalmente regulada pela Lei nº 18.331/2008. O debate sobre proteção de dados no Uruguai guarda origem com a Constituição do país, apesar dela não expressamente reconhecer um direito de proteção de

²⁸⁶ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 4. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

²⁸⁷ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 211.

²⁸⁸ KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 215 e 216.

²⁸⁹ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 32. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

dados, ou mesmo de privacidade. A Constituição do Uruguai, de 1967, não possui uma lista fechada de direitos fundamentais, apenas prevê, em seu artigo 72, que a listagem de direitos, obrigações e garantias prestadas pela Constituição não exclui outras que são inerentes à personalidade humana, ou mesmo aquelas que derivam da forma republicana de governo. Como resultado, o artigo 1º da Lei 18.331 de Proteção de Dados Pessoais e a Ação de Habeas Data estabelece expressamente que o direito à proteção de dados pessoais é inerente à pessoa humana, portanto está incluída no artigo 72.º da Constituição da República²⁹⁰.

A lei de 2008 guarda similaridade com a antiga forma da UE regular a matéria de proteção de dados pessoais, que, na época da promulgação da lei, era prescrita pela Diretiva 95/46/CE, revogada pelo RGPD. As leis nacionais sobre essa matéria na região da América Latina, em regra, são inspiradas e amplamente conectadas com a concepção e a estrutura de regulação de proteção de dados europeia, que é uma lei geral sobre o tema, a qual prescreve princípios, direitos e obrigações específicas a serem fiscalizadas por uma autoridade de controle independente. O Uruguai repete esse padrão e se conecta com a regulação da UE diante da defesa de um direito de proteção dados e do favorecimento do comércio extra fronteiriço, relevante para os países da América Latina²⁹¹. Nesse sentido, Marcelo Bauzá afirma que o sistema europeu, agora centrado no RGPD, é fonte de consulta jurídica, inspiração e adaptação de um sistema de proteção de dados no Uruguai²⁹².

Essa influência pode ser percebida no artigo da lei uruguaia sobre decisões automatizadas, que se inspirou sobremaneira no texto do art. 15(1) da Diretiva²⁹³. A lei uruguaia prevê um direito dos titulares não serem submetidos a decisões automatizadas que afetem significativamente a esfera jurídica por avaliar aspectos da sua personalidade, a exemplo das relações laborais, creditícias, e outras. Assim, cabe ao afetado impugnar as decisões tomadas por entidades públicas ou privadas que se fundamentam unicamente no tratamento de dados pessoais para definição de características de sua personalidade. Nesses casos, o texto da Lei nº 18.331 se aproxima de um direito à explicação ao garantir ao afetado pela decisão automatizada um direito de obter informação do responsável pelo tratamento sobre os critérios de valoração e o programa utilizado no tratamento.

²⁹⁰ PEHLÍVAN, Ceyhun. Data Protection in Latin America: an overview. *Global Privacy Law Review*, v. 2, n. 2. The Netherlands: Kluwer Law International BV, 2021, p. 103.

²⁹¹ BAUZÁ, Marcelo. La Ley 18.331 y el Reglamento (UE) 2016/679. *Revista Uruguaya de Protección de Datos Personales*, n. 2, 2017, p. 11.

²⁹² BAUZÁ, Marcelo. La Ley 18.331 y el Reglamento (UE) 2016/679. *Revista Uruguaya de Protección de Datos Personales*, n. 2, 2017, p. 12.

²⁹³ UNIÃO EUROPEIA. Parlamento Europeu. **Directiva 95/46/CE** do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em:

<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 10 jan. 2023.

Lei 18331, de 2008

Artigo 16

As pessoas têm o direito de não ficarem sujeitas a uma decisão com efeitos jurídicos que as afete significativamente, a qual se baseie no tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como o desempenho profissional, o crédito, a fiabilidade, o comportamento, entre outros.

O afetado pode impugnar atos administrativos ou decisões particulares que impliquem uma apreciação da sua conduta, tendo como base única o tratamento de dados pessoais que permita definir as suas características ou personalidade.

Neste caso, o afetado terá o direito de obter informações do responsável pelo banco de dados, tanto sobre os critérios de avaliação quanto sobre o programa utilizado no tratamento que serviu para adotar a decisão expressa no ato.

Figura 12 - Artigos relevantes para um direito à explicação no Uruguai (tradução livre)

Desde 2012, antes da vigência do RGPD, o Uruguai é reconhecido pela Comissão Europeia, por meio da Decisão 2012/484/UE, como um país cujo direito à proteção de dados está em conformidade com o modelo europeu, permitindo um fluxo mais facilitado de dados pessoais entre os países que fazem parte da UE e o Uruguai²⁹⁴. Essa decisão foi tomada com apoio do grupo de trabalho do Artigo 29, que, analisando especificamente o dispositivo da lei uruguaia sobre decisões automatizadas, entendeu pela conformidade desta com a Diretiva vigente. Isso porque, para o grupo de trabalho, o direito a não submissão do titular a decisões automatizadas, previsto na lei uruguaia, também é expressamente reconhecido pela Diretiva²⁹⁵.

Além disso, o terceiro parágrafo do art. 16 da lei uruguaia estabelece um princípio semelhante ao indicado no documento “*Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive*”, do grupo de trabalho. Esse parágrafo estipula que a pessoa afetada terá o direito de obter informações do controlador, tanto sobre os critérios de avaliação, quanto sobre o programa usado para processamento de dados para tomar a decisão expressa²⁹⁶. Esse direito de obter informação sobre decisões

²⁹⁴ REIGADA, Antonio Troncoso. El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional. **Revista Latinoamericana de Protección de Datos Personales**, n. 5, 2018. capítulo II.

²⁹⁵ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 3/2010 on the principle of accountability**. 2010, p. 14. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf. Acesso em: 15 mar. 2023.

²⁹⁶ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay**. 2010, p. 14. Disponível em:

automatizadas foi especificamente observado pelo grupo de trabalho para o reconhecimento do Uruguai enquanto um país conforme com as normas europeias de proteção de dados.

O direito enunciado pelo último parágrafo do art. 16 da Lei nº 18.331 pode ser percebido como uma faceta do direito à explicação, apesar de a lei não prevê-lo de forma inequívoca. Isso porque ele está previsto no escopo de incidência da lei de proteção de dados sobre as decisões automatizadas e cria uma obrigação ao responsável pelo tratamento de explicar ao interessado sobre o processo de decisão automatizado. De forma mais específica, cabe ao agente informar (i) os critérios de avaliação utilizados para tomada de decisão e (ii) sobre o programa usado. Em 2022, no intuito de orientar e facilitar o exercício de um direito à proteção de dados pelos titulares, a autoridade uruguaia, *Unidad Reguladora y de Control de Datos Personales*, publicou um guia geral sobre o tema. Neste guia, a autoridade reforça o direito de receber informações sobre decisões automatizadas nos mesmos termos da lei²⁹⁷. A legislação uruguaia não avança sobre outros critérios que devem balizar a execução desse direito, nem sobre limites aplicáveis.

Em um sentido similar à lei uruguaia de proteção de dados pessoais, o país publicou a *Estrategia de Inteligencia Artificial para el Gobierno Digital* em que elenca, no rol de princípios gerais do desenvolvimento da IA no setor público, a transparência como característica obrigatória das soluções de IA utilizadas pelo Poder Público de forma a disponibilizar os algoritmos e dados utilizados para treinamento da ferramenta e sua implementação, bem como os testes e validações realizados e tornar explicitamente visíveis, por meio de mecanismos de transparência ativa, todos os processos que utilizam IA, seja na geração de serviços públicos ou no apoio à tomada de decisões²⁹⁸.

De forma geral, os países da América Latina e Caribe que possuem princípios e marcos éticos de IA no setor público citam especificamente a transparência e a explicabilidade, porém o Uruguai não segue esse padrão. Isso não quer dizer que a explicação não seja aplicável no sistema uruguaio, já que a estratégia menciona uma transparência ativa, de forma que o princípio da explicabilidade poderia se prestar a uma interpretação mais

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf. Acesso em: 10 jan. 2023.

²⁹⁷ URUGUAI. Unidad Reguladora y de Control de Datos Personales. **Guía General de Protección de Datos Personales en Uruguay**. 2022, p. 18. Disponível em:

<https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-general-proteccion-datos-personales-uruguay>. Acesso em: 10 jan. 2023.

²⁹⁸ AGESIC. **Estrategia de Inteligencia Artificial para el Gobierno Digital**. 2022, p. 9. Disponível em:

https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-el-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Estrategia_IA%20-%20versi%C3%B3n%20espa%C3%B1ol.pdf. Acesso em: 10 jan. 2023.

ampla²⁹⁹. Ainda, a estratégia cita, em sua lista de objetivos, a definição de normas, guias e recomendações para análise de impacto, monitoramento e auditoria dos algoritmos de tomada de decisão utilizados na Administração Pública, bem como para sua interpretabilidade e explicabilidade³⁰⁰. Dessa forma, é possível perceber certa convergência entre a estratégia do país para desenvolvimento da IA no setor público e a lei de proteção de dados, ao mesmo tempo as duas situações são pouco concretas ou mesmo direcionadas para a prática de explicar as decisões automatizadas em casos não abstratos.

Diante dessa falta de maiores orientações normativas, chama atenção certo desalinhamento entre a norma e as ferramentas de proteção efetivas ao titular ou mesmo o estabelecimento de uma cultura de proteção de dados. Segundo Ana Nogrères, o número de ações iniciadas pelos titulares para proteger os seus dados pessoais é mínimo, mesmo em vista do sistema de proteção de dados uruguaio, e a falta de questionamento poderia indicar que o sistema funciona fluentemente³⁰¹. Porém, a autora destaca que nem sempre este parâmetro de avaliação é correto, porque o cidadão uruguaio médio não possui o grau de informação necessário para tomar conhecimento do risco que corre se não realizar um controle adequado, pessoal e consciente sobre quem coleta seus dados, para que finalidade, com quem serão compartilhados, como esses dados são protegidos de terceiros, e quem será responsável por sua segurança³⁰².

Assim, apenas um cidadão bem informado poderia exercer de forma adequada seus direitos previstos em leis de proteção de dados, como direito de requerer explicações sobre uma decisão automatizada. Nos casos em que o titular não possui consciência sobre o papel da proteção de dados nas suas escolhas diárias, ele encontra-se incapacitado de defender seus interesses e exercer seus direitos³⁰³. Esse risco é aprofundado em um contexto de *big data*, em que é difícil mapear os dados pessoais utilizados na tomada de decisão automatizada, ao mesmo tempo é fácil utilizá-los para formação de perfis e outras finalidades que podem limitar o acesso a bens e serviços pelos titulares. Ao mesmo tempo, diante da complexidade

²⁹⁹ OCDE. **Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe**. Paris: OECD Publishing, 2022, p. 80.

³⁰⁰ AGESIC. **Estrategia de Inteligencia Artificial para el Gobierno Digital**. 2022, p. 14. Disponível em: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-el-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Estrategia_IA%20-%20versi%C3%B3n%20espa%C3%B1ol.pdf. Acesso em: 10 jan. 2023.

³⁰¹ NOUGRÈRES, Ana Brian. El sistema legal uruguayo de protección de datos personales. **Revista de Derecho, Comunicaciones y Nuevas Tecnologías**, 2007, p. 26.

³⁰² NOUGRÈRES, Ana Brian. El sistema legal uruguayo de protección de datos personales. **Revista de Derecho, Comunicaciones y Nuevas Tecnologías**, 2007, p. 26.

³⁰³ NOUGRÈRES, Ana Brian. El sistema legal uruguayo de protección de datos personales. **Revista de Derecho, Comunicaciones y Nuevas Tecnologías**, 2007, p. 27.

dos sistemas, é importante destacar que um nível adequado de consciência sobre o tratamento de dados não é alcançado pela simples publicação do código fonte dos sistemas, como feito pelo governo uruguaio no aplicativo Coronavirus UY³⁰⁴, mas é um mecanismo de proporcionar maior transparência para os sujeitos submetidos às decisões automatizadas ou pessoas interessadas com conhecimento técnico para a análise³⁰⁵.

Apesar da lei uruguaia prever de forma mais específica um direito do titular conhecer os critérios de avaliação utilizados na tomada de decisão e o programa aplicado durante o processo, mesmo que de forma tímida, o tema ainda não foi tratado especificamente pela comunidade acadêmica e a autoridade de proteção de dados, *Unidad Reguladora y de Control de Datos Personales*, não publicou algum guia ou conteúdo sobre o tema³⁰⁶. Dessa forma, é possível afirmar pela existência de um direito à explicação na letra da Lei nº 18.331, porém não existem debates consolidados sobre sua extensão, fronteiras ou formas de execução. A lei é abstrata e não define o sentido do que seriam os critérios de avaliação e os programas utilizados em decisões automatizadas, bem como o momento e forma de transmitir essa informação.

5.2.3. Colômbia: Lei nº 1.581, de 2012

A lei geral de proteção de dados pessoais da Colômbia, Lei nº 1.581, de 2012, assim como o RGPD e a Lei nº 18.331, do Uruguai, dispõe sobre princípios de proteção de dados, direitos de titulares, deveres dos responsáveis pelo tratamento, além de mecanismos para sancionamento e fiscalização feita por uma autoridade de proteção de dados. Na Colômbia, a autoridade de proteção de dados encarregada de fiscalizar o cumprimento da lei é a *Superintendencia Industria y Comercio*. Ela não possui nenhuma publicação específica sobre decisões automatizadas de dados pessoais, porém, enquanto entidade membro da *Red Iberoamericana de Protección de Datos*, replicou um documento intitulado *Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial*. Neste relatório, a rede

³⁰⁴ URUGUAI. Ministério de Salud Publica. **Información sobre la Aplicación Coronavirus UY**. 2020. Disponível em:

<https://www.gub.uy/ministerio-salud-publica/politicas-y-gestion/informacion-sobre-aplicacion-coronavirus>.

Acesso em: 10 jan. 2023.

³⁰⁵ FUENTES, Patricio Velasco; VENTURINI, Jamila. **Decisões automatizadas na gestão pública na América Latina**. 2021, p. 27. Disponível em:

https://www.derechosdigitales.org/wp-content/uploads/08_Informe-Comparado-PT_180222.pdf. Acesso em: 16 dez. 2022.

³⁰⁶ A *Unidad Reguladora y de Control de Datos Personales* não possui publicações específicas sobre decisões automatizadas baseadas em dados pessoais, efeitos, salvaguardas, perfilamento, direito à explicação, ou mesmo sobre a incidência do art. 16 da lei de proteção de dados do Uruguai. Ainda, não foram encontrados artigos acadêmicos voltados ao tema no contexto uruguaio em buscadores como Google, Google Scholar e SciELO Uruguai.

destaca a existência de um direito à explicação sobre a decisão tomada sempre que o titular for submetido a uma decisão automatizada³⁰⁷. Porém, ao contrário dessas normativas, a lei colombiana não regula o tratamento de dados em decisões automatizadas de forma específica, nem para criar salvaguardas, ou derrogar prerrogativas ao titular. Dessa forma, na Colômbia, o tratamento de dados pessoais que se utiliza de ferramentas automatizadas com base em dados pessoais para tomar decisões não conta com direcionamentos específicos.

Para além da lei geral, existem leis colombianas esparsas aplicáveis a temas específicos. A título de exemplo, a Lei 1.266, de 2008, é uma lei setorial que regulamenta questões relacionadas ao Habeas Data e a tratamento de dados existentes em bases de dados, particularmente bases financeiras, creditícias, comerciais e de serviços. Essa lei, por mais que disponha sobre informações creditícias, setor que se vale sobremaneira de decisões automatizadas com base em dados pessoais, não regula as decisões automatizadas. Remolina Angarita destaca que os direitos relacionados a essa forma de tratamento de dados pessoais são relevantes para a pessoa afetada, já que permitiria que ela contestasse a decisão tomada com base em informações que não correspondam à realidade ou apresentasse informações ou alegações adicionais com vista à defesa dos seus direitos ou interesses, o que não está assegurado ao titular colombiano na forma da Lei 1.266³⁰⁸.

De forma geral, a lei colombiana prevê o princípio da transparência no tratamento de dados pessoais, mas, em sua qualificação, o limita a um dever do responsável pelo tratamento informar a existência de dados pessoais do titular, escopo expressivamente limitado, se comparado com as outras regulações analisadas nesta pesquisa, como a do Brasil ou da UE. Ainda, a lei define a extensão do direito de informação do titular ser apenas sobre: (i) o tratamento de dados pessoais e a finalidade; (ii) o caráter facultativo da coleta de dados sensíveis ou de crianças e adolescentes; (iii) os direitos do titular; (iv) e a identificação do responsável pelo tratamento, nada especificando sobre os dados pessoais levados em consideração ou mesmo o funcionamento de sistemas de decisão automatizada.

³⁰⁷ RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. **Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial**. 2019, p. 21. Disponível em: [https://www.sic.gov.co/sites/default/files/files/pdf/2%20RIPD%20\(2019\)%20GENERAL%20RECOMMENDATIONS%20FOR%20THE%20PROCESSING%20OF%20PERSONAL%20DATA%20IN%20ARTIFICIAL%20INTELLIGENCE\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/2%20RIPD%20(2019)%20GENERAL%20RECOMMENDATIONS%20FOR%20THE%20PROCESSING%20OF%20PERSONAL%20DATA%20IN%20ARTIFICIAL%20INTELLIGENCE(1).pdf). Acesso em: 11.02.2023.

³⁰⁸ REMOLINA-ANGARITA, Nelson. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz de estándar europeo?. **Revista Colombiana de Derecho Internacional**, n. 16, p. 489-524, 2010.

Lei 1581, de 2012

Artigo 4º

Princípios para o tratamento de dados pessoais.

e) Princípio da transparência: No Tratamento, deve ser garantido o direito do Titular de obter do Responsável pelo Tratamento ou do Gestor do Tratamento, a qualquer momento e sem restrições, informação sobre a existência de dados que lhe digam respeito;

Artigo 8º

O Titular dos dados pessoais terá os seguintes direitos:

c) Ser informado pelo Encarregado do Tratamento ou pelo Encarregado do Tratamento, a seu pedido, sobre a utilização que tem sido dada aos seus dados pessoais;

Artigo 12

O Responsável pelo Tratamento, ao solicitar autorização ao Titular, deverá informá-lo clara e expressamente do seguinte:

a) O Tratamento a que serão submetidos os seus dados pessoais e a sua finalidade;

b) O carácter facultativo da resposta às questões colocadas, quando estas sejam sobre dados sensíveis ou sobre dados de crianças e adolescentes;

c) Os direitos que o assistem como Titular;

d) A identificação, morada física ou eletrônica e número de telefone do Responsável pelo Tratamento.

Figura 13 - Artigos relevantes para um direito à explicação na Colômbia (tradução livre)

Diante desses dispositivos, é possível afirmar que a lei colombiana de proteção de dados pessoais não regula especificamente as decisões automatizadas tomadas com base em informações pessoais e, com isso, não prevê um direito à explicação. As previsões de transparência e direito de informação, além de não serem específicas para decisões automatizadas, não criam obrigações contundentes sobre a necessidade de informar o interessado sobre critérios ou mesmo a estrutura dos sistemas de tomada de decisão. Dessa forma, pelo ponto de vista de proteção de dados, o titular sujeito a esta norma não encontra-se tutelado por um direito à explicação.

A falta de orientações jurídicas não impede que sistemas de IA sejam utilizados por entidades privadas ou públicas. As iniciativas deste setor estão compiladas em repositórios que visam informar sobre a existência desses sistemas, mas não fornecem informações básicas

sobre os algoritmos³⁰⁹. Os repositórios não fornecem informações sistemáticas sobre se os sistemas usam ou não dados pessoais, como obtêm os dados usados, como operam, os resultados obtidos, quem o desenvolveu e quem é o responsável pelo tratamento. Por mais que não haja uma obrigação legal de informação, os dados acima são necessários para determinar o nível de explicabilidade das decisões do sistema, considerado aspecto fundamental no desenvolvimento dessa tecnologia³¹⁰.

Para Zabala Leal, a produção legislativa e jurídica da Colômbia deixou de lado preocupações com a ética e os efeitos jurídicos do desenvolvimento de novas tecnologias, como a IA. Como consequência, não existiriam bases normativas que sirvam de fonte para a solução de conflitos derivados do uso de produtos desenvolvidos a partir da IA no país³¹¹. Diante deste cenário, a sociedade civil organizada da Colômbia recomenda maior desenvolvimento doutrinário, regulatório, legal ou jurisprudencial sobre o tratamento de dados que ocorra por meio da tomada de decisão automatizada, a fim de que seja objeto de maiores garantias do que as oferecidas pela Lei nº 1.581, de 2012³¹².

Do ponto de vista de regulação de IA, para além da proteção de dados, a *Consejería Presidencial para asuntos económicos y transformación digital* publicou um marco ético para a Inteligência Artificial na Colômbia em que avança sobremaneira no tema de explicabilidade diante das aplicações de IA³¹³. Este marco destaca a explicabilidade como um princípio que deve guiar o desenvolvimento de IA no país enquanto complementar ao princípio da transparência, mas que busca tornar o conteúdo das informações e a forma como elas são apresentadas facilmente acessíveis. As principais informações seriam relativas aos objetivos

³⁰⁹ GUTIÉRREZ, Juan David; MUÑOZ-CADENA, Sarah. Sistemas de decisión automatizada implementados por el Estado Colombiano. **XI Congreso Internacional en Gobierno, Administración y Políticas Públicas GIGAPP**, Madrid, España, del 21 al 23 de septiembre de 2022, p. 12.

³¹⁰ GUTIÉRREZ, Juan David; MUÑOZ-CADENA, Sarah. Sistemas de decisión automatizada implementados por el Estado Colombiano. **XI Congreso Internacional en Gobierno, Administración y Políticas Públicas GIGAPP**, Madrid, España, del 21 al 23 de septiembre de 2022, p. 13. VÁSQUEZ, Carolina Sánchez. **El derecho al control humano en la inteligencia artificial**. Una propuesta de regulación del control humano como un nuevo derecho en el ordenamiento jurídico colombiano. Universidad EAFIT, 2021, p. 60. PONT, Vivian Newman; ARANGO, María Paula Àngel. **Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital**. 2019, p. 66. Disponível em: <https://www.dejusticia.org/wp-content/uploads/2019/01/Rendicio%CC%81n-de-cuentas-de-Google-y-otros-negocios-en-Colombia.pdf>. Acesso em: 11 jan. 2023.

³¹¹ ZABALA LEAL, Tatiana Dulima. La ética en inteligencia artificial desde la perspectiva del Derecho. **Via Inveniendi Et Iudicandi**, v. 16, n. 2, 2021.

³¹² PONT, Vivian Newman; ARANGO, María Paula Àngel. **Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital**. 2019, p. 96. Disponível em: <https://www.dejusticia.org/wp-content/uploads/2019/01/Rendicio%CC%81n-de-cuentas-de-Google-y-otros-negocios-en-Colombia.pdf>. Acesso em: 11 jan. 2023.

³¹³ COLÔMBIA. *Consejería Presidencial para Asuntos Económicos y Transformación Digital*. **Marco Ético para la Inteligencia Artificial en Colombia**. 2020. Disponível em: <https://www.usergioarboleda.edu.co/wp-content/uploads/2021/11/Marco-etico-para-la-inteligencia-artificial-en-Colombia-Maestria-en-Inteligencia-artificial.pdf>. Acesso em: 11 jan. 2023.

iniciais do sistemas, os resultados esperados e obtidos, considerando as complexidades que cercam a tecnologia³¹⁴. Com isso, nota-se que as normas colombianas de proteção de dados não apresentam um direito à explicação, nem em sua forma mais primária, associada à transparência e informação, mas as publicações sobre desenvolvimento da IA estão atentas a esta previsão.

5.3. Um direito à explicação em decisões automatizadas baseadas em dados pessoais na LGPD

Além do fundamento da autodeterminação informativa, dos princípios da LGPD, e dos direitos dos titulares, o controlador de dados que atua sob incidência da LGPD e se utiliza de decisões automatizadas baseadas em dados pessoais com impacto aos interesses do titular também deve observar o disposto no art. 20 da lei. No *caput*, como já detalhado, é previsto o direito de revisão da decisão, já o §1º determina o direito à explicação ao explicitar a obrigação do controlador em informar os critérios e procedimentos utilizados para a decisão automatizada, observados os segredos comerciais aplicáveis. No caso brasileiro, em comparação ao Colombiano, há uma definição específica para os casos em que o titular está sujeito a uma decisão sem interferência humana a fim de que conheça informações complementares sobre o processo de decisão para além dos dados coletados, mas também sobre a forma de utilização dos dados e os possíveis resultados a partir do tratamento.

Lei 13709, de 2018

Artigo 20

O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

³¹⁴ COLÔMBIA. Consejería Presidencial para Asuntos Económicos y Transformación Digital. **Marco Ético para la Inteligencia Artificial en Colombia**. 2020, p. 30. Disponível em: <https://www.usergioarboleda.edu.co/wp-content/uploads/2021/11/Marco-etico-para-la-inteligencia-artificial-en-Colombia-Maestria-en-Inteligencia-artificial.pdf>. Acesso em: 11 jan. 2023.

Figura 14 - Artigos relevantes para um direito à explicação no Brasil

Esse direito de conhecer informações específicas do processo de tomada de decisão automatizada, como descrito na LGPD, deve estar atento à forma da explicação, que deve ser clara e adequada, além do contexto em que se aplica. Isso porque decisões automatizadas, como apresentado no segundo tópico (tópico 2.3) desta pesquisa, estão sendo aplicadas em diversos contextos, inclusive para definir perfil³¹⁵ e permitir acesso ou não a bens, serviços e direitos fundamentais. Assim, a forma e a extensão da explicação devem estar em acordo com o sujeito e seus efeitos concretos, de modo que o direito à receber explicação ganha relevância caso essa decisão impactar funções sociais constitucionalmente protegidas, como direito à saúde, trabalho, moradia, liberdade de expressão, entre outros³¹⁶.

Traçando um paralelo com o GDPR, é possível perceber que o §1º do art. 20 não especifica o sujeito do direito à explicação, como faz no *caput* do artigo e o RGPD, que, em uma interpretação literal, limita a incidência desse direito aos titulares de dados sujeitos à decisão. Essa não especificação, somado ao fato de que sistemas de decisões automatizadas, em regra, são aplicados de forma massiva, pode indicar para um direito que pode ser exercido por outros interessados potencialmente impactados pela decisão. Por outro lado, o RGPD não limita o direito de explicar a um critério de requisição, ao contrário da LGPD, que cria a obrigação de explicar o sistema após solicitação do interessado. As discussões sobre uma explicação específica a uma decisão individual ou sistemática também não foram definidas na lei brasileira, sendo possível os dois modelos.

Para além da definição pela existência ou não de um direito à explicação, surgem diversas questões sobre a forma de alcançá-lo, ou seja, sobre a definição de parâmetros objetivos que indiquem para uma explicação suficiente ou não, como apresentado no primeiro subtópico deste tópico (tópico 5.1). Diante do desafios de se concretizar um direito à explicação, é possível defender-se que “o parâmetro a ser buscado é a inteligibilidade e explicação dos aspectos fundamentais da decisão automatizada: o seu propósito, os seus

³¹⁵ ZANATTA, Rafael. **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. 2019, p. 3 Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais?channel=doi&linkId=5c7078f8a6fdcc4715941ed7&showFulltext=true. Acesso em: 23 mar. 2023.

³¹⁶ MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência artificial e a lei de proteção de dados pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: FRAZÃO, Ana. MULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019, p. 273.

inputs, os seus resultados e os critérios e fundamentos para o julgamento”³¹⁷. Esses aspectos também estão presentes na Figura 10 - Checklist do direito à explicação. A partir desses elementos mínimos, o direito à explicação pode ser percebido como efetivo aos interesses dos interessados, já que funciona como instrumento de “ampliação do poder de barganha dos indivíduos com garantias e qualificadores que buscam conferir maior equilíbrio às assimetrias”³¹⁸. Essa dimensão individual de um direito à explicação também pode ser complementada com mecanismos de dimensão coletiva e estrutural, como será detalhado no próximo tópico (tópico 6.3).

Está expressa no §1º, do art. 20, da LGPD, a incidência dos limites do segredo de negócio na definição do que deve ser explicado, este ponto será melhor trabalhado no próximo tópico (tópico 6.2) desta pesquisa. Essa determinação, à primeira vista, restringe o conteúdo a ser informado ao interessado a título de explicação sobre o sistema automatizado sempre que a informação versar sobre segredo de negócio. No entanto, isso não significa que o controlador pode se valer dessa justificativa para negar explicação, sua utilização só “poderia ser cogitada em casos excepcionais e devidamente justificados, sob pena de esvaziar por completo diversos dos princípios da própria LGPD”³¹⁹. Uma forma de lidar com a proteção do segredo de negócio está prevista no art. 206, da Lei de Propriedade Intelectual, que, atento ao interesse dos empresários, prevê uma proteção às informações que se caracterizarem como segredo de indústria, comércio ou negócio, podendo ser reveladas em processo judicial, que seguirá em segredo de justiça, sendo vedado o uso dessas informações para outras finalidades. A imposição do segredo de negócio como limitador da extensão desse direito também está em debate na tramitação do PL nº 21/2020, em que os especialistas, durante as audiências públicas e contribuições por escritos, divergiram sobre ser o segredo de negócio um direito das empresas que pode se sobrepor ou restringir o direito das pessoas³²⁰.

Quando o argumento do segredo comercial ou industrial for utilizado para não fornecer explicações, a LGPD determina que a ANPD poderá realizar auditorias para a

³¹⁷ FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais Fundamentos da LGPD**. 1. ed. Rio de Janeiro: Forense, 2022, p. 340.

³¹⁸ ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 183.

³¹⁹ FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais Fundamentos da LGPD**. 1. ed. Rio de Janeiro: Forense, 2022, p. 343.

³²⁰ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 244 a 246.

verificação de aspectos discriminatórios no tratamento automatizado de dados pessoais, em acordo com o §2º do art. 20. É importante notar que, assim como previsto no art. 58(1)(b)(e) do RGPD, a autoridade brasileira, apoiada no art. 55-J, tem competência para realizar auditorias em situações que houver descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso. Dessa forma, essa pesquisa discorda das interpretações que indicam para uma capacidade de auditoria limitada à ANPD, a qual estaria restrita aos casos de recusa do controlador em fornecer a explicação solicitada, sob o fundamento de segredo comercial e indústria³²¹. Isso porque a ANPD poderá realizar auditorias no âmbito de sua atividade de fiscalização, isso inclui casos em que houver descumprimento à legislação de forma geral, não restrita apenas ao fundamento de segredo comercial, sendo o §2º, do art. 20, um completo do art. 55-J, XVI, da LGPD. Nesse sentido, o §2º apenas especifica a competência da ANPD de realizar auditorias em casos de indícios de tratamentos indevidos, que abarca casos de tratamentos discriminatórios.

No sistema normativo brasileiro, outras normas e documentos de orientação do governo são relevantes para a definição de um direito à explicação. O art. 5º, IV e V, da LCP determina expressamente um direito de informação ao cadastrado sobre principais elementos e critérios considerados para a análise de risco e sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento. Com base nesses direitos, o cadastrado passa a conhecer, ter explicado, de forma mais específica, sobre o sistema que foi submetido para avaliação de crédito.

Um direito à explicação já havia sido reconhecido pelo STJ que culminou com a publicação da Súmula 550, em que o tribunal entende pela possibilidade do uso de *score* de crédito, desde que o consumidor possa solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. Além disso, o art. 1º, §3º, da lei também prevê a proibição de anotar informações sensíveis para fins de concessão de crédito, como a origem étnica, orientação sexual, convicções políticas, religiosas e filosóficas, e informações de saúde e genética, de forma a preservar o cadastrado a tratamentos discriminatórios. Diante desse contexto fático e desse nível de proteção jurídica, Renato Monteiro entende que a espinha dorsal do direito à explicação de decisões

³²¹ LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, v. 26, p. 227-246, out./dez. 2020, p. 246.

automatizadas é formada a partir da combinação de um direito à transparência e da não discriminação³²².

De maneira mais abrangente, o CDC, em seu art. 6º, III, determina um direito de informação aos consumidores sobre os produtos e serviços, indicando especialmente as características e riscos que apresentam, corroborando para o desenvolvimento de uma relação de consumo informada e baseada na boa-fé. Somado a isso, o art. 43 do código apresenta um direito dos consumidores acessarem informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. Esses direitos à informação e ao acesso a dados pessoais podem ser percebidos como primeiras expressões de um direito à explicação, porém ainda limitado ao contexto de consumo e sem previsões sobre o processo automatizado em si, que segue uma lógica específica e relevante para os interesses das pessoas sujeitas a essas determinações.

Em suma, no Brasil, o direito à explicação é especificamente previsto na lei de proteção de dados, ao contrário da lei da Colômbia sobre a matéria, e está atento aos interesses do titular, que são protegidos de forma mais contundente que a lei do Uruguai, a qual prevê explicações apenas sobre os critérios de avaliação e o programa utilizado pelo controlador de dados no processo de tomada de decisão automatizada. A definição de critérios e procedimentos, somado às construções doutrinárias e jurisprudenciais sobre o tema, são relevantes para a sedimentação teórica desse direito e consequente desenvolvimento prático. Ao mesmo tempo, os desafios que circundam a implementação desse direito ainda são expressivos, especialmente quando se leva em conta ou busca-se extrair a razão de ser de um direito de receber explicações sobre decisões automatizadas que afetam a esfera de direitos ou interesses dos envolvidos.

6. OS LIMITES DO DIREITO À EXPLICAÇÃO NA GARANTIA À AUTODETERMINAÇÃO INFORMATIVA

Apesar da falta de parâmetros e mecanismos de execução prática do direito à explicação, esse direito possui um papel relevante na concretização do fundamento da autodeterminação informativa. Isso não significa que ele seja suficiente para garantir o controle do titular sobre a forma de tratamento dos seus dados pessoais nos processos automatizados. Por isso, faz-se necessário compreender os limites desse direito na execução da autodeterminação enquanto um dos conceitos originários e fundamentais para tutela da

³²² MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**, Artigo Estratégico, n. 39, 2018, p. 8.

proteção de dados. A partir disso, é possível endereçar outras ferramentas da matéria para suprimir as lacunas de uma explicação em um mundo o qual as decisões que impactam a vida das pessoas cada vez mais estão sendo realizadas de forma automatizada.

As barreiras do direito à explicação estão diretamente ligadas à complexidade técnica do sistema, de forma a ser mais difícil explicar modelos algorítmicos que utilizam um volume expressivo de dados, métodos diferentes de treinamento, técnicas complexas de processamento, entre outros elementos. É mais simples explicar aplicações que utilizam poucas variáveis de entrada (*inputs*) e as combinam de maneiras relativamente diretas, como aproximar e distanciar as associações de causa e efeito³²³. É nesse sentido que acadêmicos percebem uma escolha mutuamente excludente, um *trade-off*, entre explicabilidade e performance do sistema³²⁴.

Além disso, a explicação pode ser formulada por duas categorias com objetivos diferentes: uma centrada no modelo e outra centrada no assunto. A primeira fornece informações mais amplas sobre o sistema sem considerar um *input* específico, de forma a destacar o comportamento computacional para considerar as motivações e o contexto de implementação do modelo, os dados de treinamento, e a performance do processamento dos dados³²⁵. Já a segunda categoria permite uma explicação local, restrita aos dados de *input* específicos, e só pode ser garantida após a tomada de decisão, já que depende dos dados de entrada para explicar a solução final³²⁶.

A categoria centrada no assunto pode ser considerada mais atraente por permitir tornar evidente a construção de modelos mentais mais eficazes e relevantes, os quais geram confiança justificada e permite desenvolvimento eficiente dos sistemas algorítmicos³²⁷. Edwards e Veale entendem que o RGPD indica para uma explicação de uma decisão específica (explicação baseada no assunto) em vez de uma visão geral vaga de um modelo complexo (explicação baseada no modelo)³²⁸. Por outro lado, é importante destacar que, apesar dessa diferenciação, as duas formas de explicação parecem ser válidas por cumprirem

³²³ EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a “right to explanation” is probably not the remedy you are looking for. **Duke Law and Technology Review**, v. 16, n. 1, 2017, p. 59.

³²⁴ KOZYRKOV, Cassie. **Explainable AI won't deliver. Here's why**. 2018. Disponível em: <https://kozyrkov.medium.com/explainable-ai-wont-deliver-here-s-why-6738f54216be>. Acesso em: 16 jan. 2023.

³²⁵ EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a “right to explanation” is probably not the remedy you are looking for. **Duke Law and Technology Review**, v. 16, n. 1, 2017, p. 55.

³²⁶ EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a “right to explanation” is probably not the remedy you are looking for. **Duke Law and Technology Review**, v. 16, n. 1, 2017, p. 56.

³²⁷ EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a “right to explanation” is probably not the remedy you are looking for. **Duke Law and Technology Review**, v. 16, n. 1, 2017, p. 62.

³²⁸ EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”? **IEEE Security & Privacy**, v. 16, n. 3, 2018, p. 5.

com um direito à explicação, como previsto nas leis de proteção de dados, já que não definem por uma das categorias.

Associado a esses limites, é possível perceber algumas barreiras para a concretização de um direito à explicação na garantia da autodeterminação informativa, mesmo em seu sentido não tradicional. Em vista do volume de pessoas afetadas pelas decisões automatizadas e do impacto desta para o cotidiano moderno, torna-se fulcral que os interessados sejam considerados nesse processo automatizado. Para tanto, explicações específicas sobre o processo de decisão permitem que os interessados participem contextualmente e se oponham de maneira informada ao resultado final, inclusive redistribuindo as relações de poder estabelecidas. Ao mesmo tempo, existem limitações que não podem ser ignoradas, como a falta de visibilidade sobre as informações relevantes, o desenvolvimento de ferramentas explicáveis, a proteção do segredo de negócio, bem como o próprio tratamento automatizado de dados no contexto do *big data*, como será evidenciado nos tópicos a seguir.

6.1. Barreiras da transparência

Uma das limitações do direito à explicação é justamente o seu alcance enquanto uma faceta da transparência. Em regra, medidas de transparência estão associadas a outras atividades que passam a ser possíveis a partir da informações divulgadas, como a participação dos interessados na ação informada, a oposição e questionamento sobre a decisão tomada, a supervisão e controle dessa ação³²⁹. O fundamento da transparência ganha ainda mais força nos atos de interesse público, em que, por meio da obrigação de publicidade e transparência, o Poder Público permite controle externo sobre a legalidade e legitimidade das suas ações, como disposto no art. 37 da CF.

No âmbito privado, cada vez é mais forte a ideia de que empresas as quais tomam decisões relevantes para um grupo de consumidores devem não apenas tornar suas decisões compreensíveis ao seu corpo técnico. A obrigação de informar também tem como destinatário os gestores de risco e reguladores, para que seja possível confirmar as informações utilizadas na tomada de decisões³³⁰. Assim, a transparência é mecanismo utilizado para gerar confiança e prestação de contas naqueles contextos em que há assimetria de poder entre o agente que promove a transparência e aquele que recebe as informações. As pessoas submetidas àquele

³²⁹ ARNANZ, Alba. Decisiones Automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos. **Revista de Derecho Público: Teoría y Método**, v. 3, 2021. capítulo 1.3.1. Transparencia y justificación de las decisiones públicas automatizadas.

³³⁰ PASQUALE, Frank. Restoring transparency to automated authority. **Journal on Telecommunication and High Technology Law**, v. 9, n. 235, 2011, p. 256.

sistema transparente possuem ferramentas para questioná-lo e verificar a sua conformidade com o objetivo buscado.

No entanto, a transparência por si só pode ser um mecanismo limitado. Um primeiro desafio é o risco da transparência ser utilizada para ocultar informação, é possível que o conteúdo relevante para o titular fique inadvertidamente escondido nos volumosos "entulhos" de informações tornadas visíveis³³¹. Nesse cenário, os titulares são bombardeados com centenas de páginas de políticas de privacidade, relatórios longos sobre tratamento de dados, documentos de governança, mas que não tornam os titulares mais conscientes e conhecedores do processo que estão sujeitos. Essa falta de clareza não intencional ou inadvertida é resultado da indefinição de limites informacionais, temporais ou estruturais que normalmente existem para gerenciar o fluxo de informação³³². Como consequência, as pessoas passam a ignorar deliberadamente o conteúdo elaborado para garantir transparência da decisão automatizada.

O momento em que os mecanismos de transparência são disponibilizados ou desenvolvidos importa no resultado final. Isso porque a transparência pode ter uma relevância futura, significar uma divulgação antecipada ou contínua, ou mesmo dar visibilidade após o sistema ser aplicado. Como consequência, diferentes momentos no tempo podem exigir ou produzir diferentes tipos de responsabilidade e necessidade de transparência do sistema³³³. Além disso, a dimensão temporal da transparência é complexificada quando versa sobre sistemas de aprendizado de máquinas. Esses sistemas são conhecidos por aprenderem à medida que aumentam a quantidade e os tipos de dados de entrada, o número de titulares de dados e forma com que eles interagem com o sistema³³⁴. Por isso, a definição da extensão da explicação dos sistemas deve estar atenta ao momento em que as ferramentas de transparência são utilizadas para que estejam em acordo com o modelo utilizado.

Em regra, esse esforço para trazer mais transparência no processo de tratamento de dados ocorre na divulgação de avisos ou políticas de privacidade. Porém, na prática, esses documentos de governança pouco contribuem para um nível de informação devida e efetiva aos interessados. Isso porque, em regra, eles não são lidos pelos titulares, são longos e escritos

³³¹ STOHL, Cynthia; STOHL, Michael; LEONARDI, Paul. Digital Age Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age. **International Journal of Communication**, [S.l.], v. 10, p. 15, jan. 2016. ISSN 1932-8036. Date accessed: 16 jan. 2023, p. 133.

³³² STOHL, Cynthia; STOHL, Michael; LEONARDI, Paul M. Digital Age Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age. **International Journal of Communication**, [S.l.], v. 10, p. 15, jan. 2016. ISSN 1932-8036. Date accessed: 16 jan. 2023, p. 133.

³³³ ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New media and society**, v. 20, n. 3, p. 973-989, 2018, p. 982.

³³⁴ ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New media and society**, v. 20, n. 3, p. 973-989, 2018, p. 982.

de maneira pouco acessível.³³⁵ As pessoas geralmente não entendem as informações recebidas sobre seus dados e, com isso, não ocupam posição para tomar decisões ponderadas sobre custo-benefício de se sujeitar a determinado tratamento de dados³³⁶. Ou ainda, se leem o documento, muitas vezes as pessoas carecem de conhecimento prévio suficiente para fazer uma escolha informada com base na explicação, ou ainda sua escolha pode ser distorcida por várias dificuldades de tomada de decisão³³⁷.

Tendo à disposição volume expressivo de informação, inclusive sobre decisões automatizadas, cria-se uma noção de fadiga, em que o titular recebe volume expressivo de informações, mas não consegue focar no conteúdo que é relevante para seus interesses. Essa prática de usar os mecanismos de transparência para ocultar informações chama ainda mais atenção diante dos requisitos de um direito à explicação. Não há definição taxativa de quais informações devem ser garantidas para concretizar esse direito e é necessário um requerimento do titular para que ele acesse essas informações. Nesses casos, há menor incentivo para a transparência ativa, em que o controlador, de pronto, atende alguns requisitos do direito à explicação e este pode publicar informações irrelevantes e não úteis para que o titular conheça elementos do processo de decisão.

Diante das obrigações de transparência determinadas pelas regulações de proteção de dados, Helen Nissenbaum destacou a existência de um paradoxo da transparência. Segundo a autora, é improvável que se atinja uma transparência do significado textual e uma transparência da prática, quando se tem um não se tem outro³³⁸. Isso porque a informação considerada de forma específica, estanque, não está de acordo com um contexto mais amplo e impede que pessoas possam compreender os riscos de efeitos colaterais e procedimentos falhos no contexto. Em regra, a transparência não é sinônimo de confiança, já que as pessoas se sentem confortáveis mesmo quando submetidas a sistemas que não conhecem. Nesse sentido, para além da transparência, as pessoas se baseiam em expectativas e confiam no conhecimento técnico dos profissionais, na supervisão de entidades de fiscalização, e, sobretudo, o interesse do sistema, qualquer que seja a sua origem, pelo bem-estar humano³³⁹.

³³⁵ FOWLER, Geoffrey. **I tried to read all my app privacy policies. It was 1 million words**. 2022. Disponível em: <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>. Acesso em: 13 jun. 2023.

³³⁶ SOLOVE, Daniel. The Limitations of Privacy Rights. **GW Law Faculty Publications and Other Works**, 2022, p. 20.

³³⁷ SOLOVE, Daniel. Privacy Self-Management and the consent Dilemma. **Harvard Law Review**, v. 126, 2013, p. 1888.

³³⁸ NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus. Journal of the American Academy of Arts and Sciences**, v. 140, n. 4, 2011, p. 36.

³³⁹ NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus. Journal of the American Academy of Arts and Sciences**, v. 140, n. 4, 2011, p. 36

O objetivo de determinar obrigações de transparência e um direito à explicação é garantir que o titular possa escolher de forma livre e autônoma, concretizando, assim, o fundamento da autodeterminação informativa. Porém, transparência não é sinônimo de que a pessoa irá decidir autonomamente a partir dessas informações. Na verdade, existe um paradoxo em que, mesmo quando as pessoas entendem os documentos de transparência, elas não são informadas de maneira relevante sobre as decisões que estão submetidas³⁴⁰. Ananny e Crawford afirmam que a transparência é uma forma limitada de conhecer os sistemas e não pode ser usada para explicar um conjunto de sistemas que utilizam dados produzidos por agentes humanos e não humanos cujo significado não reside internamente, mas relacionalmente³⁴¹.

Além da falta de definição sobre a extensão jurídica do direito à explicação, a informação fornecida sobre as decisões automatizadas podem não ser adequadas àqueles que as solicitam. Para além da apresentação de explicações que levem em consideração o contexto sócio-econômico do interessado, deve-se observar a razoabilidade daquelas decisões em que se solicitou explicações. É razoável supor que pessoas as quais buscam entender o sistema provavelmente obtiveram decisões que não concordam. Com isso, é mais provável que elas tenham fornecido *inputs* os quais podem genuinamente ser considerados anômalos em comparação aos dados de treinamento do sistema algorítmico³⁴². Como resultado, essas pessoas estariam fora do padrão de casos os quais o sistema foi treinado e pode bem explicar, logo é provável a explicação ser falha nas situações em que as pessoas mais precisam dela.

A divulgação de detalhes do processo de tomada de decisão para atender requisitos de transparência pode colocar em risco os próprios sistemas, como no caso de modelos desenvolvidos para identificar agentes fraudulentos. Informar extensivamente os mecanismos utilizados para garantir segurança de um sistema pode dar ferramentas para esses agentes manipularem os sistemas e impedirem seu bom funcionamento³⁴³. Garantir ampla transparência sobre os sistemas pode ameaçar a própria proteção de dados e vulnerabilizar certos grupos, a exemplo da divulgação dos dados pessoais utilizados no treinamento de um sistema como a justificativa de explicar como ele foi desenvolvido. Essa prática teria como

³⁴⁰ BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. In: LANE, Julia *et al.* **Privacy, Big Data, and the Public Good: frameworks for engagement**. Cambridge: Cambridge University Press, 2014, p. 59.

³⁴¹ ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New media and society**, v. 20, n. 3, p. 973-989, 2018, p. 984.

³⁴² EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a "right to explanation" is probably not the remedy you are looking for. **Duke Law and Technology Review**, v. 16, n. 1, 2017, p. 60

³⁴³ ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New media and society**, v. 20, n. 3, p. 973-989, 2018, p. 978.

consequência a exposição de dados pessoais de forma inadequada para o atendimento da finalidade daquela divulgação.

Um exemplo dessa barreira à transparência foi objeto de análise da corte de primeira instância do distrito de Hague, nos Países Baixos. Duas associações de caçadores e atiradores holandeses impugnaram o uso de um questionário digital elaborado para avaliar, em nota de 0 a 10, as condições psicológicas do titular para receber uma licença de uso de arma. Em vista do dever de explicar o processo de tomada de decisão automatizada a partir do questionário, caberia ao órgão que utiliza esse questionário demonstrar conformidade com suas obrigações. Especificamente sobre o direito à explicação, a corte decidiu que as informações relevantes sobre o algoritmo não devem ser compartilhadas com os requerentes, já que a divulgação poderia prejudicar a efetividade do questionário. Por exemplo, seria possível que, conhecendo a forma de avaliação, os requerentes “enganassem” o algoritmo para dar pontuações favoráveis a eles³⁴⁴. Para a corte, os autores não precisam da entrega destes documentos para atingirem o fim a que se propõem, tendo em vista que o Estado prometeu colaborar com a realização de relatórios preliminares, com as garantias associadas de confidencialidade³⁴⁵.

Portanto, o direito à explicação concretizado apenas pelas ferramentas de transparência não são suficientes para garantia de uma autodeterminação informativa diante de suas limitações. Destaca-se a falta de parâmetros específicos para a execução desse direito, pela sobrecarga de informação, ou mesmo pelo ocultamento de informação relevante para o exercício da autonomia do titular. A transparência, quando não concretizada de forma adequada, também cria riscos para os titulares de dados e para o sistema.

6.2. Ferramentas explicáveis

Outra limitação do direito à explicação diz respeito à própria viabilidade de gerar explicações sobre o processo de tomada de decisão. Uma das formas tradicionais de explicar as decisões é a partir dos dados de entrada utilizados para se chegar ao resultado final, existe uma ideia comum de que é adequado explicar sistemas de IA a partir de uma avaliação de causalidades³⁴⁶. No entanto, Talia Gillis entende que informar sobre os *inputs* não é suficiente

³⁴⁴ PAÍSES BAIXOS. RB Den Haag. CC/09/585239/ KG ZA 19/1221. Julgado em: 11.02.2020. Disponível em: https://gdprhub.eu/index.php?title=Rb._Den_Haag_-_C/09/585239/_KG_ZA_19/1221. Acesso em: 16.02.2023.

³⁴⁵ PAÍSES BAIXOS. RB Den Haag. CC/09/585239/ KG ZA 19/1221. Julgado em: 11.02.2020. Disponível em: https://gdprhub.eu/index.php?title=Rb._Den_Haag_-_C/09/585239/_KG_ZA_19/1221. Acesso em: 16.02.2023.

³⁴⁶ FRAZÃO, Ana. **Decisões algorítmicas e direito à explicação**. Em que medida é possível encontrar explicações em decisões algorítmicas? 2021. Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2021-11-24-Decisoes_algoritmicas_e_direito_a_explicacao_Em_que_medida_e_possivel_encontrar_explicacoes_em_decisoes_algoritmicas.pdf. Acesso em: 11 nov 2022.

para proteção do titular e pode, inclusive, potencializar resultados discriminatórios, de forma a indicar para uma falácia sobre os dados de entrada³⁴⁷. Em sua pesquisa, Gillis demonstra que o controle dos dados os quais podem ser utilizados como *inputs*, especialmente nos sistemas de proteção ao crédito, não auxilia a endereçar o risco de discriminação. Isso porque o controle, ou mesmo a proibição, de dados de entrada pode funcionar como uma arma que fortalece o *status quo* do contexto em que aquela decisão é aplicada. No contexto de crédito, isso significa minar a promessa de preços de crédito algorítmicos para criar um mercado de crédito mais inclusivo³⁴⁸.

Dessa forma, para evitar-se cenários de discriminação, uma abordagem que se debruça sobre os resultados do sistema pode ser adequada, já que, por meio de testes com as decisões finais, é possível perceber os *tradeoffs* que o sistema necessariamente enfrenta³⁴⁹. É nesse sentido que os itens em vermelho da Figura 10 - Checklist do direito à explicação foram formulados. Eles dão visibilidade para os parâmetros levados em conta no resultado por meio de comparações com outras decisões similares, bem como a capacidade de previsão do sistema quando exposto a dados diversos e as propriedades não desejadas. Uma análise focada no resultado permite compreender de que forma as decisões algorítmicas estão impactando os interessados e contribuindo para o aprofundamento de um resultado discriminatório³⁵⁰. Essa dificuldade de controlar os dados de entrada também está associada ao contexto de *big data*, em que é possível realizar correlações e combinações de um volume expressivo de dados, questão que será desenvolvida no subtópico a seguir (tópico 6.3).

Diante desses impasses, o campo da XAI, como destacado no tópico anterior (tópico 5.1), foi desenvolvido para que, além da explicação humana, fosse possível implementar sistemas de IA explicáveis a partir de algumas abordagens. As abordagens comuns versam sobre explicação por texto, imagem, área de interesse, exemplo, simplificação e relevância de uma *feature*³⁵¹. Dada a performance, complexidade e escalabilidade do sistema, as abordagens de XAI podem ser mais eficazes para apresentar explicações, mas variam de acordo com o objetivo da explicação buscada e da própria decisão formulada. A título de exemplo, as abordagens de relevância de *feature* fornecem explicações medindo quantitativamente a

³⁴⁷ GILIS, Talia B. The Input Fallacy. *Minnesota Law Review*. 2021, p. 2. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571266. Acesso em: 17 jan. 2023.

³⁴⁸ GILIS, Talia B. The Input Fallacy. *Minnesota Law Review*. 2021, p. 7. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571266. Acesso em: 17 jan. 2023.

³⁴⁹ GILIS, Talia B. The Input Fallacy. *Minnesota Law Review*. 2021, p. 8. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571266. Acesso em: 17 jan. 2023.

³⁵⁰ GILIS, Talia B. The Input Fallacy. *Minnesota Law Review*. 2021, p. 78. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571266. Acesso em: 17 jan. 2023.

³⁵¹ BELLE, Vaishak; PAPANTONIS, Ioannis. Principles and Practice of Explainable Machine Learning. *Frontiers in Big Data*, v. 4, 2021, p. 4.

importância de um *feature*, já as abordagens de simplificação de modelo constroem padrões relativamente simples como um "representante intermediário" (*proxy*) para os opacos³⁵².

Em vista de uma preocupação comum entre os usuários de redes sociais e formuladores de políticas sobre publicidade direcionada, o Facebook introduziu o botão "Por que estou vendo isso?". Essa funcionalidade fornece aos usuários uma explicação sobre o motivo pelo qual foi mostrado a eles um determinado anúncio. À primeira vista, esse botão pareceu ser um mecanismo de transparência interessante para o usuário compreender como seus dados pessoais são utilizados pelas plataformas de publicidade.

No entanto, uma pesquisa demonstrou que a forma como as explicações dos anúncios do Facebook, a qual apresenta apenas o atributo mais prevacente, pode permitir que anunciantes maliciosos ofusquem facilmente as explicações discriminatórias ou as quais visem atributos sensíveis à privacidade. Andreou e outros pesquisadores indicam que as explicações dos anúncios do Facebook sugerem que atributos os quais nunca foram especificados pelo anunciante podem ter sido selecionados como explicações válidas. Isso tornaria essas explicações potencialmente enganosas para os usuários finais sobre quais eram os parâmetros de segmentação do anunciante³⁵³.

Por outro lado, conceber a XAI ou as ferramentas de explicação como única forma de tornar os sistemas de IA confiáveis pode não estar em conformidade com a realidade. Cassie Kozyrkov destaca que a IA é útil para automatizar o inefável, ou seja, aquilo que não se pode descrever. Isso torna difícil a explicação sobre o funcionamento do próprio sistema, que processa dados sem instruções explícitas ou não se limita a elas. Dessa forma, a confiança na IA não dependeria da explicação que o sistema ou seus desenvolvedores dão sobre seu funcionamento, mas sim do treinamento a que foi submetido. A testagem do sistema seria a forma de garantir sua segurança mais eficiente que a elaboração de explicações. Muitas vezes explicações podem ser simplistas, incompletas e, assim, incorretas, em vista da complexidade do sistema, já que a IA tem sido utilizada para desempenhar atividades ainda não solucionadas ou prescritas de forma simples pelo humano³⁵⁴.

A partir do defendido por Kozyrkov e das barreiras da transparência (tópico 6.1), é razoável concluir que apenas a explicação do sistema não é suficiente para que ele seja

³⁵² BELLE, Vaishak; PAPANTONIS, Ioannis. Principles and Practice of Explainable Machine Learning. **Frontiers in Big Data**, v. 4, 2021, p. 13.

³⁵³ ANDREOU, Athanasios et al. Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations. Network and Distributed Systems Security (NDSS) Symposium 2018, 18-21 February 2018, San Diego, CA, USA. ISBN 1-1891562-49-5.

³⁵⁴ KOZYRKOV, Cassie. **Explainable AI won't deliver. Here's why.** 2018. Disponível em: <https://kozyrkov.medium.com/explainable-ai-wont-deliver-here-s-why-6738f54216be>. Acesso em: 17 jan. 2023.

confiável para os parâmetros de proteção de dados. O mesmo se repete no fundamento da autodeterminação informativa, em que os mecanismos de explicação de decisão automatizada não são suficientes, ao mesmo tempo que outras ferramentas podem ser complementares para concretizar esse fundamento. Esse entendimento também leva em consideração a opacidade técnica e a falta de conexões causais para tomada de decisão, já destacadas anteriormente (tópico 2.4).

Existe uma movimentação nacional e internacional de regulação da ferramenta utilizada para maior parte das decisões automatizadas, a IA, como descrito no tópico anterior (tópico 5.1). Essa foi uma saída para enfrentamento dos desafios impostos pela IA de uma forma geral, não apenas em aplicações específicas, como no tratamento de dados pessoais, regulada pela LGPD, ou para a definição de pontuação de crédito, orientada pela LCP, por exemplo. Por meio de um marco legal para desenvolvimento da IA, seria possível estabelecer direitos e outros mecanismos para proteção do elo vulnerável da relação entre a máquina e o humano, envolvendo, inclusive, programadores, desenvolvedores, fornecedores e usuários. Ainda, uma regulação poderia prever a implementação de “ferramentas de governança e de um arranjo institucional de fiscalização e supervisão, criar condições de previsibilidade acerca da sua interpretação e, em última análise, segurança jurídica para inovação e o desenvolvimento econômico-tecnológico”³⁵⁵.

No âmbito nacional, estão tramitando, no Senado Federal, os PL nº 5051/2019, 21/2020, 872/2021 e 2338/2023. Esses PL visam regular o uso de IA de forma geral, ou seja, aplicável a diferentes contextos os quais a ferramenta pode ser útil, desde a área de negócios e comércio, à área da saúde, educação, e acesso a serviços e bens públicos. Para tanto, a última minuta de texto, apresentada pela Comissão de Juristas como substitutivo, destaca que a regulamentação deve observar os potenciais riscos da ferramenta, de forma a intervenção regulatória ser mais enfática em cenários de externalidades negativas concretas e excessivas³⁵⁶. Essa abordagem de risco também é percebida a nível internacional, em propostas de regulação sobre o tema, como a proposta da UE de *Artificial Intelligence Act*³⁵⁷.

³⁵⁵ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 10.

³⁵⁶ BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022, p. 12.

³⁵⁷ UNIÃO EUROPEIA. Comissão Europeia. **EU AI Act**. 2021. Disponível em: <https://artificialintelligenceact.eu/the-act/>. Acesso: 22 nov. 2022. Outros documentos internacionais também buscam construir uma estrutura regulatória para a IA, mas sem endereçar soluções para uma jurisdição, apenas

Ao mesmo tempo, a maturidade do debate e a eficácia de um marco normativo sobre o assunto devem ser levados em conta, já que regras sobre IA implicam na definição de incentivos ou não para o desenvolvimento da tecnologia. A definição de normas sobre IA inefetivas podem gerar maior insegurança jurídica e expor as pessoas a possíveis violações de direitos, especialmente as mais vulneráveis. Isso pode resultar em uma “solução” normativa insuficiente para os desafios concretos que a tecnologia impõe³⁵⁸. Uma regulação de IA implica em um esforço de compatibilizar essa norma com o já previsto no ordenamento jurídico, inclusive o fundamento da autodeterminação informativa e o direito à explicação especificados na LGPD. Logo, a depender da norma aprovada, esse direito pode ser impactado por uma regulação geral sobre o desenvolvimento da IA no Brasil.

As ferramentas objeto do direito à explicação são, em regra, protegidas por segredo de negócio, que também podem funcionar como limite para definir o escopo do uso de ferramentas explicáveis. Os próprios controladores podem se apoiar nesse argumento para negar explicações aos titulares. De alguma forma, a própria LGPD reconheceu essa restrição no §1º, do art. 20, quando garantiu o direito à explicação, observados os segredos comercial e industrial. Essa mesma discussão está presente no debate sobre o PL nº 21/2020 e 2338/2023, os quais visam regulamentar o uso de IA no Brasil, como descrito no tópico anterior. No RGPD, o Considerando 63 aponta o segredo de negócio como uma das possibilidades de restrição do direito de acesso, que abarca esse direito à lógica da decisão automatizada. Essas disposições sobre segredo de negócio estão previstas nas normas como um elemento limitador da explicação diante de uma decisão automatizada, o que pode indicar que a proteção do segredo sempre se sobrepõe ao direito à explicação.

No entanto, o primeiro ponto de atenção é que não há uma definição sobre o que seria segredo comercial ou industrial para o contexto de proteção de dados, ou seja, são conceitos sem subsídio na LGPD. Como consequência, esse argumento poderia ser utilizado analisando-se o caso concreto³⁵⁹, já que a incidência desses argumentos não deve ocorrer de forma genérica. Atentas a essa possibilidade, as diretrizes do Grupo de Trabalho do Artigo 29 afirmam que os controladores não podem contar com a proteção de seus segredos comerciais

destacando possíveis abordagens regulatórias e pontos de atenção, como UNESCO. **d Hoc Expert Group (AHEG) for the preparation of a draft text of a recommendation on the ethics of artificial intelligence**. 2020. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000373434>. Acesso em: 11 nov. 2022. e OCDE. **OECD AI Principles**. 2019. Disponível em: <https://oecd.ai/en/ai-principles>. Acesso em: 11 nov. 2022.

³⁵⁸ MATTIUZZO, Marcela. **O carro na frente dos bois: a precipitada regulação da IA no Brasil**. 2021. Disponível em:

<https://www.jota.info/opiniao-e-analise/colunas/fronteiras-concorrenca-regulacao/precipitada-regulacao-da-inteligencia-artificial-no-brasil-26082021>. Acesso em: 17 jan. 2023.

³⁵⁹ MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**, Artigo Estratégico, n. 39, 2018, p. 14.

como desculpa para negar acesso ou recusar-se a fornecer informação ao titular dos dados³⁶⁰. Logo, o argumento do segredo de negócio é pertinente em situações excepcionais e não pode ser aplicado de forma irrestrita e indiscriminada. Não se segue a lógica do tudo ou nada de explicação, deve-se buscar um nível de explicação suficiente e adequado para o titular e para a empresa que possui direito de não revelar seus segredos de negócio.

A autoridade de proteção de dados da Áustria, *Datenschutzbehörde*, julgou um caso sobre limitação do direito à explicação diante de um segredo comercial, em 2020. No caso, o controlador de dados pessoais era responsável por calcular um *score* de marketing para identificar a qual grupo de interesse certas pessoas participavam. Um titular requereu explicações sobre o funcionamento desse sistema, que foi negado pelo controlador sob justificativa de se tratar de informações protegidas pelo segredo de negócio. A autoridade decidiu que o controlador não é obrigado a divulgar o algoritmo, código-fonte ou outro documento completo usado ao criar as pontuações de marketing. Porém, ele deve fornecer informações para os afetados no caso individual, o que torna possível a rastreabilidade, a compreensão e a correção das variáveis de entrada no caso em questão³⁶¹. Neste caso, a autoridade austríaca entendeu que o *score* de marketing é um exemplo de *profiling* e isso seria suficiente para surgir um direito à explicação, nos moldes do art. 15(1)(h), do RGPD. Para a configuração desse direito, não seria necessária a identificação de uma decisão automatizada, na moldura definida pelo art. 22³⁶². Essa é uma decisão que primou pela faceta individual e por uma explicação após a decisão, já que afirmou pelo fornecimento de informações detalhadas apenas aos afetados no caso concreto.

O método de cálculo da pontuação possui valor econômico para seus desenvolvedores e esse é objetivo de proteção do segredo de negócio. No entanto, a autoridade avalia ser baixo o risco de cópia deste método, já que fica a cargo do controlador o cumprimento de suas obrigações de explicação com o titular. Especificamente, as seguintes informações em conexão com o cálculo da pontuação devem ser evidenciadas: (i) *inputs* e como eles surgiram; (ii) efeito dos *inputs* no *score*; (iii) explicação do motivo pelo qual o titular foi atribuído a um determinado resultado de avaliação; (iv) lista de possíveis categorias de perfis ou informações equivalentes semelhantes que permitam ao titular exercer seus direitos de retificação e

³⁶⁰ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 17. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

³⁶¹ ÁUSTRIA. Datenschutzbehörde. **2020-0.436.002**. Julgado em: 08.09.2020. Disponível em: [https://gdprhub.eu/index.php?title=DSB_\(Austria\)_-2020-0.436.002](https://gdprhub.eu/index.php?title=DSB_(Austria)_-2020-0.436.002). Acesso em: 17 jan. 2023.

³⁶² ÁUSTRIA. Datenschutzbehörde. **2020-0.436.002**. Julgado em: 08.09.2020. Disponível em: [https://gdprhub.eu/index.php?title=DSB_\(Austria\)_-2020-0.436.002](https://gdprhub.eu/index.php?title=DSB_(Austria)_-2020-0.436.002). Acesso em: 17 jan. 2023.

apagamento e verificar a legalidade do processamento³⁶³. Dessa forma, a autoridade entende pela compatibilidade do segredo de negócio com o direito à explicação, sendo necessária uma análise mais detida do caso concreto e consequente explicação nos termos adequados.

O Tribunal Administrativo Regional de Viena requereu uma decisão terminativa do Tribunal de Justiça da UE sobre questões relacionadas à divulgação de informações ao titular dos dados, quando essas informações estiverem protegidas por segredos comerciais. O tribunal austríaco identificou uma tensão no caso o qual as informações necessárias para compreensão de uma decisão automatizada decorrem de um algoritmo protegido pela lei de segredos comerciais da UE. O tribunal sugeriu a possibilidade de aliviar essa tensão, divulgando as informações em questão apenas à autoridade ou tribunal relevante e permitindo que eles determinem se um segredo comercial nos termos da Diretiva 2016/943 está presente. O tribunal e autoridade também determinariam se os dados correspondentes a explicação devem ser fornecidos de acordo com o art. 15(1), do RGPD. No entanto, a questão foi enviada ao Tribunal de Justiça da UE e ainda não há decisão final³⁶⁴.

6.3. Tratamento de dados pessoais na era do Big Data

O direito à explicação, enquanto uma das facetas para concretização da autodeterminação informativa, é constantemente desafiado em um contexto de *big data*. Nesse cenário, dados são tratados de forma massiva, em diversos contextos, para diversas finalidades e, quando relacionados a pessoas, eles são utilizados sem necessariamente o conhecimento do titular. Assim, garantir que apenas o titular possui controle sobre suas informações, na concepção tradicional de autodeterminação é uma atividade de execução improvável. Como visto até aqui, o direito à explicação não busca garantir controle sobre os dados pessoais, em que o titular autoriza seu uso em todas as aplicações e para todos os agentes possíveis. Esse direito visa permitir que o titular execute seus direitos quando submetido a decisão automatizada relevante baseada em dados pessoais, diante dos efeitos dessa decisão e da possibilidade de conhecer, contestar, e solicitar revisão do resultado final.

Assim, explicar uma decisão que não usa apenas a camada de dados coletados diretamente do titular como *input* torna o cenário mais complexo. Esse é o cenário mais frequente nos tratamentos de dados que se utilizam de ferramentas automatizadas diante de um contexto de *big data*. Dados compartilhados ou cruzados, submetidos a tratamento

³⁶³ ÁUSTRIA. Datenschutzbehörde. **2020-0.436.002**. Julgado em: 08.09.2020. Disponível em: [https://gdprhub.eu/index.php?title=DSB_\(Austria\)_-_2020-0.436.002](https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2020-0.436.002). Acesso em: 17 jan. 2023.

³⁶⁴ ÁUSTRIA. Verwaltungsgericht Wien. **VGW-101/042/791/2020-44**. Julgado em: 11.02.2022. Disponível em: https://gdprhub.eu/index.php?title=VGW_-_VGW-101%2F042%2F791%2F2020-44. Acesso em: 17 jan. 2023.

secundário ou mesmo inferidos também são objetos de explicação, apesar dos agentes de tratamentos, nesses casos, possuírem uma menor relação com o titular, se comparado aos dados coletados diretamente do titular pelo primeiro controlador. Essa falta de relação entre o titular de dados e o agente de tratamento pode ter como consequência uma diminuição da expectativa do titular no tratamento realizado por agente que ele não conhece.

No caso de novas finalidades atribuídas ao tratamento, a LGPD determina que essa finalidade deve ser específica, legítima e compatível³⁶⁵ com a finalidade original (art. 6º, I). Isso se relaciona com a noção da privacidade enquanto integridade contextual³⁶⁶. Quando o consentimento for a base legal que fundamentou o tratamento, a LGPD indica que o controlador deve informar ao titular quando seus dados forem tratados para atingir finalidade não compatível com a finalidade consentida no primeiro tratamento (art. 9º, §2º). Como consequência, cabe ao controlador fazer uma análise de compatibilidade das finalidades para, com base no princípio da adequação, validar a regularidade do fluxo informacional. Essa avaliação deve levar em considerações atores que compõem a relação (controladores, operadores, titulares, grupos impactados), os tipos de informação trocadas, as expectativas e as restrições que o fluxo está submetido em vista das obrigações previstas na LGPD³⁶⁷.

Esses elementos ganham novos contornos quando resultam no tratamento automatizado de dados que se vale de informações coletadas em outros contextos não necessariamente compatíveis com a finalidade da decisão. Nesses casos, faz-se necessária análise caso a caso. A autodeterminação não determina que o titular seja capaz de controlar o fluxo informacional desde o início³⁶⁸, mas que haja elementos garantidores da integridade desse fluxo, bem como considerem os interesses e direitos dos titulares, e a capacidade de participação no fluxo. Logo, o tratamento secundário, comum no *big data*, é mais um elemento que complexifica o direito à explicação por falta de previsibilidade ao titular.

³⁶⁵ BRASIL. Autoridade Nacional de Proteção de dados. **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico_defeso_eleitoral.pdf. Acesso em: 07 mar. 2023, p. 13.

³⁶⁶ NISSENBAUM, Helen. **Privacy in context**: Technology, policy, and the integrity of social life. Bloomington: Stanford Law Books, 2009, p. 38.

³⁶⁷ ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 187.

³⁶⁸ ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 188

As decisões automatizadas também podem resultar no ato de inferir dados pessoais. Sistemas automatizados são utilizados não apenas para presumir e decidir sobre acesso a determinado serviço, produto ou oportunidade, mas também para inferir dados e características de uma pessoa, como seus hábitos e comportamentos. Diante disso, Wachter e Mittelstadt defendem a necessidade de um direito de inferências razoáveis, e não de inferências explicáveis, a ser extraído a partir das leis de proteção de dados. Para os autores, o primeiro direito seria adequado para garantir que as pessoas, individualmente consideradas, sejam capazes de gerenciar como as inferências serão elaboradas, como o nível de invasividade, antes mesmo que a decisão seja tomada³⁶⁹. A partir de um direito à inferência razoáveis, seria possível obrigar o controlador a justificar proativamente suas escolhas para análises inferenciais de alto risco antes da implantação generalizada³⁷⁰, essa seria a principal diferença para um direito à explicação. Novas ferramentas jurídicas estão sendo formadas diante de aparentes limites de um direito à explicação.

O contexto de *big data* também desafia o caráter individual do desenvolvimento tradicional da proteção de dados. As ferramentas criadas para tutelar o titular passam a não mais serem adequadas para tratamento de dados masivo e que afasta o controle individual do interessado. Os direitos estabelecidos nestas normas, em regra, são direcionados aos titulares de dados, o que contribui para a noção de que a privacidade do titular é garantida através da concretização de seus direitos. No entanto, os titulares estão frequentemente em posição de impotência e vulnerabilidade em relação aos agentes de tratamento, já que não participam ou, ao menos, conhecem o tratamento de dados pessoais os quais estão submetidos. Parece ser intuitivo dar aos indivíduos mais controle sobre seus dados pessoais com direitos de privacidade. Porém, Solove destaca que, para ser eficaz, o controle, se e na medida da sua existência, não pode ser colocado apenas nas mãos dos indivíduos, o controle deve vir da sociedade³⁷¹. Dessa forma, o âmbito de tutela da proteção de dados deixa de ser individual e passa a também existir em uma esfera coletiva.

O art. 22 da LGPD é expresso ao determinar que a defesa dos interesses e dos direitos dos titulares poderá ser exercida coletivamente. Essa previsão evidencia a tutela da proteção de dados para além do titular afetado, abrangendo inclusive decisões que impactam interesses de grupos. Esses instrumentos podem reduzir o desequilíbrio de poder existente entre os

³⁶⁹ WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age on big data and AI. **Columbia Business Law Review**. 2019, p. 79.

³⁷⁰ WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age on big data and AI. **Columbia Business Law Review**, 2019, p. 83.

³⁷¹ SOLOVE, Daniel. The Limitations of Privacy Rights. **GW Law Faculty Publications and Other Works**, 2022, p. 17.

controladores de dados e os titulares³⁷², já que passam a atuar de forma conjunta para proteção dos seus interesses. A noção coletiva da proteção de dados também é amparada na responsabilidade civil prevista na LGPD, especialmente ao reconhecer a aplicabilidade de ações de reparação por danos coletivos, no §3º, do art. 42, da lei. Esse padrão se repete no art. 52, §5º, ao determinar que o produto da arrecadação das multas aplicadas pela ANPD deve ser destinado ao Fundo de Defesa de Direitos Difusos.

Em vista do uso massivo das decisões automatizadas, essa tutela coletiva ganha ainda maior relevância. A forma com que uma decisão automatizada é tomada pode impactar os interesses de todas as outras pessoas submetidas àquele sistema e todas outras que ainda estarão sujeitas a ele. Essa abordagem também propicia a análise do impacto e de inconsistências da decisão para grupos específicos, como nos casos já abordados em que a decisão automatizada reforça discriminações a um grupo específico e diminui sua capacidade de decidir autonomamente. Portanto, a autodeterminação também é balizada por outros elementos que surgem a partir do cenário de *big data*.

7. CONCLUSÃO

Estar sujeita a decisões automatizadas é uma realidade para as pessoas, tanto no Brasil quanto no mundo. Essas decisões impactam os cidadãos em diversos contextos, como publicidade direcionada, recomendação de entretenimento, *score* de crédito, valor de seguros, atuação em aplicativo de transporte e entrega, acesso a tratamentos de saúde, educação e políticas públicas específicas. Em regra, essas decisões se baseiam em algoritmos de IA treinados de diversas formas e desenvolvidos em ferramentas de complexidade distintas que levam a resultados explicáveis em graus também diversos. Sistemas de aprendizado de máquinas inauguraram uma forma de decidir, já que permitem levar em consideração experiências de decisões anteriores, mas também perceber elementos antes não percebidos como determinantes. Diante do risco envolvido na tecnologia, a LGPD previu regras específicas para os casos em que sejam tomadas decisões automatizadas com base em dados pessoais que afetam os interesses dos titulares.

Apesar dessas definições, ainda não está sedimentado em quais casos essas decisões afetariam os titulares, dificuldade também enfrentada no contexto europeu em indicar quando a decisão automatizada faz incidir as regras criadas no RGPD. No contexto europeu, o Grupo

³⁷² MARTINS, Pedro Bastos Lobo; HOSNI, David Salim Santos. Tomada de Decisão Automatizada e a Regulamentação da Proteção de Dados: Alternativas Coletivas Oferecidas pela Lei Geral de Proteção de Dados. **Revista Internet e Sociedade**, v. 1, n. 2, dez. 2020, p. 93. Disponível em: <https://revista.internetlab.org.br/736-2/>. Acesso em: 23 mar. 2023.

de Trabalho do Artigo 29 entende que, para avaliar o impacto nos interesses do titular, deve-se considerar se a decisão (i) permite ou nega um determinado benefício social concedido por lei; (ii) limita sua liberdade de ir e vir e se associar, como a recusa da entrada de uma pessoa na fronteira, ou a sujeição a medidas de segurança acrescidas pelas autoridades competentes; ou (iv) altera seus direitos ou estado legal em um contrato, como a desconexão automática de um serviço de telefonia móvel por quebra de contrato³⁷³.

As decisões automatizadas são utilizadas para prever comportamentos humanos e formar perfis sobre os titulares. Ou seja, esses sistemas foram criados para, com base em dados pessoais, seja os expressamente informados para o controlador, seja os inferidos, dizerem quem os titulares são. Essa aplicação da tecnologia traz riscos relevantes para a proteção de dados, como evidenciado nesta pesquisa (tópico 2.4), a exemplo da vigilância, da discriminação e da opacidade desses sistemas.

A hipótese fixada nesta pesquisa, qual seja, de que existem fronteiras a um direito à explicação e a percepção da sua existência não é suficiente para garantia plena do fundamento da autodeterminação, é confirmada. Isso porque o conceito da autodeterminação está em processo de resignificação para deixar de estar associado apenas à noção de controle individual do titular e passar a estar relacionado a uma noção de poder de decisão e participação no tratamento de dados. De acordo com as ideias de Rodotà, a autodeterminação informativa não se esgotaria no exercício de um controle individual pelo titular como um fim em si mesmo, mas como uma ferramenta de realocação de poder na sociedade³⁷⁴. Um sentido similar à autodeterminação é indicada por Bruno Bioni ao apresentar o conceito de codeliberação informacional, que se opõe ao de dominação informacional e reconhece a deliberação conjunta sobre tratamento de dados³⁷⁵. É notória a mudança de sentido atribuída à autodeterminação e sua relação com equilíbrio na distribuição de poder.

Por mais que a autodeterminação informativa guarde origens no debate do consentimento, já que os dois conceitos buscam entregar o controle sobre o tratamento de dados ao titular, é importante perceber suas diferenças. No consentimento, em regra, os titulares decidem na coleta dos dados sobre se consentem com tratamento. As consequências

³⁷³ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. Bruxelas: European Commission, 2017, p. 10. Disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963. Acesso em: 14 dez. 2021.

³⁷⁴ RODOTÀ, Stefano. **A vida na sociedade da vigilância**. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

³⁷⁵ BIONI, Bruno Ricardo. **Accountability na regulação de dados pessoais: virtudes e vicissitudes**. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, 2021, p. 242.

dessa decisão não podem ser adequadamente avaliadas em uma série de transações isoladas³⁷⁶. Por outro lado, a autodeterminação informativa, em seu sentido tradicional, preocupa-se com a capacidade do titular controlar e participar de todo o processo de tratamento de dados. Com a evolução do conceito, o consentimento foi se distanciando da autodeterminação e, assim, dando espaço para obrigações de transparência, como é o caso do direito à explicação.

O sentido tradicional de autodeterminação informativa foi estruturado a partir de 1983 com a decisão do Tribunal Constitucional Federal Alemão sobre a Lei do Censo da época. A constitucionalidade dessa lei foi levada ao tribunal diante do risco que ela representava para os direitos gerais de personalidade por falta de precauções processuais e de finalidade na organização dos dados do recenseamento. O tribunal entendeu que a Lei Fundamental garantiria o poder do indivíduo de decidir por si mesmo sobre a divulgação e o uso de seus dados pessoais, que resultaria no direito à autodeterminação informativa. Assim, foi reconhecido ao cidadão um direito de não ser submetido a tratamentos de dados por terceiros que viole sua capacidade de desenvolver sua personalidade livremente.

No ordenamento jurídico brasileiro, a autodeterminação foi expressamente prevista apenas com a LGPD, porém seus efeitos já se relacionavam com outros instrumentos legais. Nesta pesquisa, destaca-se (i) a Constituição Federal, por meio dos direitos fundamentais, especialmente com o *Habeas Data*; (ii) o CDC, por determinar o direito de informação e de acesso aos dados pessoais e suas fontes quando compilados em bancos de dados e cadastros de consumidores; (iii) a LCP, a qual regula a formação de bancos de dados sobre adimplência para se evitar abusos nessa atividade; (iv) a LAI, que busca garantir o direito fundamental à informação por meio, também, da proteção da privacidade; e (v) o MCI, por afirmar um direito à proteção de dados e estabelecer o consentimento do titular e a exclusão dos dados.

Durante a tramitação da LGPD, o conceito de autodeterminação não estava presente desde as primeiras minutas da lei, apesar de ser central no desenvolvimento da matéria de proteção de dados. Mesmo com a inclusão do termo no texto em 2016, o conceito não foi objeto de controvérsia ou discussão pelos agentes envolvidos no processo legislativo.

Antes mesmo da entrada em vigor da LGPD, o STF reconheceu a existência de um direito à proteção de dados vinculado à autodeterminação informativa, tendo em vista este direito ser uma chave para interpretação do primeiro. Com isso, estabeleceu-se o objeto de proteção desses direitos, que não se limita à informações sigilosas, mas inclui qualquer tipo de dados pessoais. O julgamento brasileiro se deu em um contexto fático bastante similar ao

³⁷⁶ SOLOVE, Daniel. Privacy Self-Management and the consent Dilemma. *Harvard Law Review*, v. 126, 2013, p. 1893.

alemão, que reconheceu a autodeterminação como direito fundamental quando analisou a constitucionalidade da lei de recenseamento. No Brasil, discutiu-se a constitucionalidade de uma MP que determinava o compartilhamento de dados dos usuários do Serviço Telefônico Fixo Comutado e do Serviço Móvel Pessoal com o IBGE para a produção de estatística oficial durante a pandemia. O tribunal brasileiro fixou entendimento pela impossibilidade de compartilhamento de dados e pela existência do direito à proteção de dados, protegido por meio da fixação de salvaguardas mínimas e suficientes para a garantir direitos fundamentais.

A autodeterminação foi argumento central neste julgamento e também o é na LGPD, por ser um dos fundamentos da lei e, com isso, ser fio condutor que direciona a interpretação a ser dada às obrigações previstas nela, inclusive em relação aos seus princípios e direitos. Em vista do objeto desta pesquisa, destacou-se os seguintes princípios e direitos influenciados pela noção de autodeterminação informativa: (i) princípio de livre acesso e transparência; (ii) princípio da finalidade, necessidade e adequação; (iii) princípio da não discriminação; (iv) direito de informação e acesso; e (v) direito de revisão. Os princípios de proteção de dados, desde o início das discussões sobre a matéria, convergem para garantir ao titular ferramentas para que ele possa controlar o tratamento de dados e participar da decisão sobre como suas informações são utilizadas. Nesse sentido, os princípios e os direitos compõem dois dos pilares da proteção de dados enquanto regulação criada para proteger e dar poder aos titulares.

Os princípios da transparência e do livre acesso impõem ao agente de tratamento obrigações de, a partir de uma postura ativa, informar de maneira geral o titular sobre o tratamento de dados, principalmente ao cumprir o direito de informação e de acesso aos dados pessoais. O primeiro independe de requerimento do titular, enquanto o segundo depende. O pressuposto é que um titular que conhece o tratamento a que está submetido possui armas para se autodeterminar, perceber abusos e exercer seus outros direitos. A transparência é uma das formas de diminuir o desequilíbrio informacional, e, conseqüentemente, de poder entre os agentes e as pessoas impactadas. O objetivo do direito à informação é fazer com que as pessoas melhorem a forma com que tomam decisões³⁷⁷. Assim, o nível e a forma de transparência devem se adequar às circunstâncias do tratamento, inclusive considerando a relação entre os envolvidos e as capacidades de compreensão do grupo de titulares afetados.

O direito de revisão permite que o titular solicite a reanálise daquela decisão automatizada, inclusive para que o resultado final seja alterado. Para que o titular possa verificar a efetividade da revisão, ele deve conhecer o sistema, seja a partir das informações

³⁷⁷ SOLOVE, Daniel. *The Limitations of Privacy Rights*. **GW Law Faculty Publications and Other Works**, 2022, p. 19.

prestadas diante do princípio da transparência, seja por meio dos dados pessoais indicados como consequência do princípio do livre acesso e do direito de acesso aos dados. O direito de revisão também é instrumentalizado a partir das explicações sobre o sistema, já que os fundamentos de um pedido de revisão são evidenciados a partir de explicações sobre o funcionamento do sistema. O direito à explicação é pressuposto do direito de revisão, por meio da obrigação de explicação é que o titular ganha poder de contestar de forma específica e fundamentada e pedir revisão de uma decisão.

Todo tratamento de dados está vinculado a uma finalidade legítima, específica, explícita e informada para que seja válido e possa ser realizado. Ainda, se a finalidade for válida, mas o objeto do tratamento for excessivo, para além do essencial à finalidade almejada, o tratamento viola o princípio da necessidade. Se a finalidade for válida e os dados imprescindíveis para alcançá-la, mas o tratamento não for compatível com a finalidade informada ao titular, o princípio da adequação é infringido. Já o princípio da não discriminação preserva os interesses do titular, posto que a capacidade de se autodeterminar quando está exposto a tratamentos discriminatórios abusivos ou ilícitos é expressivamente reduzida, diante do desequilíbrio de poder em prejuízo do titular. Para que esse princípio seja observado, é fundamental que sejam definidas as discriminações abusivas, tendo em vista ser um conceito flexível e adaptável a diversas situações. Os princípios da prevenção, responsabilização e prestação de contas criam obrigações aos agentes de tratamento justamente para que, em vista do risco da atividade, demonstrem a implementação de medidas eficazes para atestar a conformidade do tratamento ao prescrito em lei.

A concretização desses princípios e direitos é ainda mais desafiadora em um cenário de sistemas opacos, em que há pouca transparência sobre a forma de tratamento de dados, bem como os critérios técnicos levados em consideração e seus efeitos na sociedade. O *big data* também tensiona esses dispositivos ao permitir o processamento de volume expressivo de dados pessoais, mesmo sem considerar o contexto e a finalidade que foram coletados no primeiro momento. Grande quantidade de dados e poder de processamento auxiliam inclusive na formação de perfis de comportamento e produção de dados inferidos, que não necessariamente estão de acordo com os interesses dos titulares.

É nesse contexto que surge a necessidade de positivação de um direito à explicação, especialmente quando titulares estão sujeitos a sistemas de decisões automatizadas baseadas em seus dados pessoais e com impacto nos seus interesses. No Brasil, esse direito está expresso no §1º, do art. 20, da LGPD. Na UE, Uruguai e Colômbia, um direito similar a esse está previsto nas leis de proteção de dados em diferentes níveis de concretização.

O RGPD estabelece uma obrigação dos controladores apresentarem informações úteis relativas à lógica do sistema automatizado, bem como à importância e consequências do tratamento. Nesse contexto, há debate acadêmico expressivo sobre a operacionalização desse direito, como (i) a existência de um dever de explicar; (ii) a extensão desse direito e as informações necessárias para explicar uma decisão; (iii) a relação entre esse direito e os outros direitos do titular; (iv) o momento da explicação, se ela deve ser anterior ou posterior à decisão, de forma a dar poder de escolha para o titular decidir sobre a pertinência do tratamento, ou de garantir a ele uma explicação específica sobre o resultado final aplicado no seu caso concreto; (v) bem como outras medidas de transparência complementarem a obrigação explicar as decisões, como o RIPD e a possibilidade de auditoria feita pela autoridade de proteção de dados.

Já o Uruguai possui uma legislação inspirada na Diretiva 95/46/CE, que foi revogada pelo RGPD, em que cria o direito do afetado pela decisão automatizada obter informações do responsável pelo banco de dados sobre critérios de avaliação e o programa utilizado. Assim como o RGPD, a lei do Uruguai determina direito geral dos titulares não serem submetidos a decisões automatizadas que afetem seus interesses. Essas previsões legais sobre decisões automatizadas foram especialmente consideradas pela Comissão Europeia na decisão sobre a possibilidade de transferência internacional de dados para o país. Isso destaca a relevância do tema para avaliação do sistema de proteção de dados pela Comissão Europeia. A obrigação de informar, prevista na lei do Uruguai, é uma faceta do direito à explicação, apesar de a lei não prevê-lo de forma inequívoca. Uma determinação explícita apenas consta na *Estrategia de Inteligencia Artificial para el Gobierno Digital* do país.

A lei de proteção de dados da Colômbia não regula especificamente os casos de decisões automatizadas, nem para criar salvaguardas, ou derogar prerrogativas ao titular. Ela apenas apresenta o princípio da transparência e o direito de ser informado sobre a utilização dos dados pessoais, sem especificar alguma informação aplicável ao contexto das decisões automatizadas. Diante deste cenário, a sociedade civil organizada da Colômbia percebe a necessidade de um desenvolvimento doutrinário, regulatório, legal ou jurisprudencial sobre o tratamento de dados por meio da tomada de decisão automatizada. Assim como o Uruguai, o poder executivo publicou um marco ético sobre IA em que prevê a explicabilidade enquanto um dos pressupostos para desenvolvimento da tecnologia.

Apesar das diversas formas de regular um direito à explicação, é comum que este direito guarde origem no princípio da transparência e no direito de informação. Estes são dispositivos fundamentais no desenvolvimento da matéria de proteção de dados pessoais,

desde os FIPP. Conhecer o processo de decisão permite que os titulares intervenham na decisão³⁷⁸, se oponham de forma fundamentada ao resultado final, além de estar informado sobre de que forma seus dados serão utilizados e impactaram na personalidade do titular.

Não existe uma fórmula rígida do momento em que esse direito deve ser atendido, se apenas após a decisão automatizada, de modo que a explicação leve em consideração as nuances do caso concreto, ou se ele pode ser concretizado anteriormente sem informar individualmente as explicações do caso concreto. Na LGPD, a obrigação de explicar os critérios e procedimentos utilizados para a decisão surge após a solicitação do interessado. Apesar disso, toda informação garantida ao titular deve ser contextual, em linguagem simples, acessível e com conteúdo relevante, para que, assim, o desequilíbrio de poder entre o agente de tratamento e o afetado seja minimizado. Uma das questões ainda não definida é o destinatário desses direitos, em vista do impacto massivo do tratamento de dados e seu aspecto coletivo, o que torna os titulares interessados no processo, mas não apenas eles, como também a sociedade civil organizada e grupos afetados de forma específica.

Dessa forma, o direito à explicação permite que os outros direitos dos titulares se concretizem, como o direito de revisão da decisão, de correção de dados desatualizados ou mesmo da eliminação de dados desnecessários, excessivos ou tratados em desconformidade. A autodeterminação informativa, enquanto um dos fundamentos da matéria de proteção de dados, é reafirmada em uma lógica de explicação. Sem ela, o titular passa a não ter ferramentas de controle sobre seus dados quando utilizados em decisões automatizadas, de forma a afetar seu livre desenvolvimento da personalidade. Os novos sentidos atribuídos à autodeterminação corroboram com a ideia de um maior equilíbrio de poder detido pelos agentes que manipulam as informações, inclusive pessoais. A explicação se mostra como uma ferramenta atual para se alcançar esse fundamento, em vista da disseminação de sistemas de decisão automatizada e do impacto desses para os direitos e liberdades dos afetados.

Ainda não há definição unânime da extensão de um direito à explicação. A matéria da explicação deve variar de acordo com o caso concreto, com os impactos da decisão para o titular, bem como os riscos envolvidos. A partir desses requisitos, esta pesquisa elaborou a Figura 10 - Checklist do direito à explicação para evidenciar parâmetros já estabelecidos pela doutrina no sentido de garantir uma explicação ao titular, seja ela mais simples, destacados na caixa verde, ou mais robustos, delineados nas caixas laranja e vermelha. Em regra, uma explicação adequada é garantida nos casos em que o tratamento de dados é resultado de

³⁷⁸ GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”. *AI MAGAZINE*, 2017, p. 55.

decisão automatizada e se sabe quais os dados pessoais, os parâmetros e as ponderações feitas pelo sistema. Ainda, é relevante saber o impacto da decisão nos interesses do afetado, os riscos envolvidos no sistema, e quais mudanças nos dados pessoais de entrada teriam alterado o resultado final da decisão.

No entanto, essa explicação pode não ser suficiente para que o titular possa se autodeterminar em um contexto de disseminação de sistemas complexos de IA e *big data*. Os limites do direito à explicação na garantia do fundamento da autodeterminação devem ser observados. Esse direito é apenas mais uma das ferramentas estabelecidas nas normas de proteção de dados que permite, especificamente, o entendimento e a oposição das decisões automatizadas. Outros mecanismos, como o RIPD, auditorias feitas pela autoridade³⁷⁹, soluções de governança de dados, proteção de dados por design³⁸⁰ e teste nos sistemas de IA³⁸¹, se mostram complementares para a garantia da autodeterminação. Além de não ser o único, o direito à explicação encontra limites expressivos na concretização desse fundamento ao, por exemplo, impor ao titular um ônus excessivo de depender dele a requisição de explicações sobre a decisão. Como consequência, na falta de uma cultura de proteção de dados, existe o risco desse direito ser concretizado apenas por grupo específico de pessoas que conhecem o ciclo de vida de seus dados, e não titulares comuns³⁸².

O próprio sistema de IA impõe limitações para o direito à explicação, mas que não invalidam esse direito. As ferramentas de tomada de decisão automatizada devem ser transparentes para com os titulares de acordo com o contexto de sua aplicação, os interesses deles e os riscos envolvidos na aplicação do sistema. No entanto, essa transparência pode gerar cenário de ocultação de informação, fadiga na quantidade de documentos fornecidos e falha na comunicação com os interessados sobre o impacto do sistema. Especificamente sobre o conteúdo da transparência, a simples informação sobre os dados de *input* já se mostrou incapaz de garantir explicações analíticas sobre o funcionamento do sistema e um possível efeito discriminatório. Com isso, explicações por meio de testes se mostram ferramenta útil

³⁷⁹ CASEY, Bryan; FARHANGI, Ashkon; VOGLP, Roland. Rethinking explainable machines: the GDPR's right to explanation debate and the rise of algorithm audits in enterprise. **Berkeley Technology Law Journal**, v. 34, 2019, p. 169.

³⁸⁰ CASEY, Bryan; FARHANGI, Ashkon; VOGLP, Roland. Rethinking explainable machines: the GDPR's right to explanation debate and the rise of algorithm audits in enterprise. **Berkeley Technology Law Journal**, v. 34, 2019, p. 179.

³⁸¹ ESTADOS UNIDOS DA AMÉRICA. **Preparing for the future of artificial intelligence**. 2016. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf. Acesso em: 22 nov. 2022.

³⁸² EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”? **IEEE Security & Privacy**, v. 16, n. 3, 2018, p. 6.

para concretizar o direito à explicação. Outra barreira é a proteção do segredo de negócio, que, à primeira vista, poderia impedir o conhecimento do sistema, porém há certa indefinição do escopo dessa proteção, de forma a ser possível uma interpretação restritiva desse conceito.

O direito à explicação está previsto no cenário brasileiro e é uma das facetas do fundamento da autodeterminação informativa, mesmo diante de seus novos sentidos. Esse direito é pressuposto para a concretização de outros direitos de proteção de dados quando a pessoa é sujeita a decisões automatizadas, como o de oposição, atualização dos dados e revisão do resultado final. Ao mesmo tempo, esse direito não é suficiente para tutelar a proteção de dados dos interessados frente aos novos desafios do *big data* e dos sistemas de IA, à dimensão coletiva da proteção de dados, ao paradoxo da transparência e do impacto das decisões automatizadas, seja inferindo dados pessoais³⁸³, realizando previsões ou determinando escolhas dos afetados. Esse direito encontra fronteiras inclusive na concretização da autodeterminação enquanto um direito de personalidade, o que indica para as limitações da própria matéria de proteção de dados pessoais, em vista das iminentes barreiras culturais, éticas e técnicas. Esses elementos são agenda para uma nova pesquisa que se debruce inclusive sobre um devido processo informacional³⁸⁴, tendo em vista que os debates sobre um eventual direito à explicação sobre a decisão convergem para ideia de *fairness*, igualdade, autonomia e não discriminação no resultado.

³⁸³ WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age on big data and AI. **Columbia Business Law Review**. 2019, p. 85.

³⁸⁴ CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. **Boston College Law Review**, vol. 55, 2014.

REFERÊNCIAS

- AGESIC. **Estrategia de Inteligencia Artificial para el Gobierno Digital**. 2022, p. 9. Disponível em: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Estrategia_IA%20-%20versi%C3%B3n%20espa%C3%B1ol.pdf. Acesso em: 10 jan. 2023.
- ALEMANHA. **Lei Fundamental da República da Alemanha**. 1949. Disponível em: <https://www.btg-bestellservice.de/pdf/80208000.pdf>. Acesso: 11 nov. 2022.
- ALEMANHA. **Volkszählungsgesetz 1983**. 1983. Disponível em: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBI&start=//*/%5B@attr_id=%27bgbl182s0369.pdf%27%5D#_bgbl_%2F%2F*%5B%40attr_id%3D%27bgbl182s0369.pdf%27%5D_1668075101860. Acesso em: 11 nov. 2022.
- ALEMANHA. Entscheidungen der amtlichen Sammlung 65, 1 (71), **Recenseamento**. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 11 nov. 2022.
- ALEMANHA. Entscheidungen der amtlichen Sammlung 54, 148 (155), **Eppler**. Disponível em: <https://www.servat.unibe.ch/dfr/bv054148.html>. Acesso em: 10 nov. 2022.
- ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020.
- ALIMONTI, Veridiana. **Algoritmos e autodeterminação: uma contribuição a partir das noções de autodeterminação informativa e controle no contexto de decisões automatizadas**. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, 2022.
- ANDERSON, Chris. **The Long Tail**. 2004. Disponível em: <https://www.wired.com/2004/10/tail/>. Acesso em: 28 dez. 2022.
- ANDREOU, Athanasios *et al.* Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations. **Network and Distributed Systems Security (NDSS) Symposium 2018**, 18-21 February 2018, San Diego, CA, USA. ISBN 1-1891562-49-5.
- ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New media and society**, v. 20, n. 3, p. 973-989, 2018.
- ARAUJO, Theo *et al.* In AI we trust? Perceptions about automated decision-making by artificial intelligence. **AI & Society**, v. 35, p. 611-623, 2020.
- ARCHEGAS, João Victor. **Proteção de Dados e Transparência em Moderação de Conteúdo na Europa, Reino Unido e Brasil**. 2021. Disponível em: <https://itsrio.org/wp-content/uploads/2021/07/Protecao-de-Dados-e-Transparencia-em-Moderacao-de-Conte%C3%BAdo.pdf>. Acesso em: 28 dez. 2022.
- ARNANZ, Alba. Decisiones Automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos. **Revista de Derecho Público: Teoría y Método**, v. 3, 2021.
- ARRIETA, Alejandro *et al.* Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. **Information Fusion**, Volume 58, 2020, Pages 82-115, ISSN 1566-2535.
- ÁUSTRIA. Datenschutzbehörde. **2020-0.436.002**. Julgado em: 08.09.2020. Disponível em: [https://gdprhub.eu/index.php?title=DSB_\(Austria\)_-2020-0.436.002](https://gdprhub.eu/index.php?title=DSB_(Austria)_-2020-0.436.002). Acesso em: 17 jan. 2023.

ÁUSTRIA. Verwaltungsgericht Wien. **VGW-101/042/791/2020-44**. Julgado em: 11.02.2022. Disponível em: [https://gdprhub.eu/index.php?title=VGW - VGW-101%2F042%2F791%2F2020-44](https://gdprhub.eu/index.php?title=VGW_-_VGW-101%2F042%2F791%2F2020-44). Acesso em: 17 jan. 2023.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. In: LANE, Julia *et al.* **Privacy, Big Data, and the Public Good: frameworks for engagement**. Cambridge: Cambridge University Press, 2014.

BAUZÁ, Marcelo. La Ley 18.331 y el Reglamento (UE) 2016/679. **Revista Uruguaya de Protección de Datos Personales**, n. 2, 2017.

BELLE, Vaishak; PAPANTONIS, Ioannis. Principles and Practice of Explainable Machine Learning. **Frontiers in Big Data**, v. 4, 2021.

BENNETT, Colin. **Regulating privacy: data protection and public policy in Europe and the United States**. New York: Cornell University, 1992.

BIBAL, Adrien, LOGNOUL, Michael, DE STREEL, Alexandre *et al.* Legal requirements on explainability in machine learning. **Artificial Intelligence Law** **29**, 149–169. 2021. Disponível em: <https://doi.org/10.1007/s10506-020-09270-4>. Acesso em: 15 dez. 2022.

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

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana. MULHOLLAND, Caitlin (coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019.

BIONI, Bruno Ricardo. **Accountability na regulação de dados pessoais: virtudes e vicissitudes**. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, 2021.

BOLDYREVA, Elena; GRISHINA, Natalia; DUISEMBINA, Yekaterina. Cambridge Analytica: ethics and online manipulation with decision-making process. **The European Proceedings of Social & Behavioural Sciences**, dez., 2018.

BRADFORD, Anu. The Brussels Effect. **Northwestern University Law Review**, v. 107, n. 1, 2012.

BRASIL. Ministério da Justiça. **Cultura Digital**. 2010. Disponível em: <http://pensando.mj.gov.br/dadospessoais2011/debata-a-norma/>. Acesso em: 14 nov. 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.168.547/RJ**. Relator Ministro Luis Felipe Salomão. 2010. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencia_l=959347&num_registro=200702529083&data=20110207&formato=PDF. Acesso em: 16 nov. 2022.

BRASIL. Câmara dos Deputados. **Inteiro Teor PL 40460/2012**. 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012. Acesso em: 14 nov. 2022.

BRASIL. Ministério da Justiça. **Consulta Pública - Anteprojeto de Lei para a Proteção de Dados Pessoais**. Pensando o Direito. 2015. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-d-e-dados-pessoais/>. Acesso: 13 nov. 2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5.276/2016**. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459. Acesso em: 13 nov. 2022.

BRASIL. Câmara dos Deputados. **Requerimento n. 5.017/2016**. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1484640. Acesso em: 14 nov. 2022.

BRASIL. Câmara dos Deputados. **Comissão especial destinada a proferir parecer ao projeto de lei nº 4060, de 2012**. 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305. Acesso em: 14 nov. 2022.

BRASIL. Ministério da Justiça e Segurança Pública. **Decolar.com é multada por prática de geo pricing e geo blocking**. 2018. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/collective-nitf-content-51>. Acesso em: 02 jan. 2022.

BRASIL. Presidência da República. **Mensagem nº 451, de 14 de agosto de 2018**. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 14 nov. 2022.

BRASIL. Senado Federal. **Relatório legislativo CAE**. 2018. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7751914&ts=1630450894215>. Acesso em: 14 nov. 2022.

BRASIL. Congresso Nacional. **Estudo do Veto nº 24/2019**. 2019. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7977991&ts=1630423600906&disposition=inline>. Acesso em: 12 dez. 2022.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 16 nov. 2022.

BRASIL. Ministério da Cidadania. **Auxílio Emergencial 2020**. 2020. Disponível em: <https://aplicacoes.cidadania.gov.br/vis/data3/index.php?g=2>. Acesso em: 12 dez. 2022.

BRASIL. Autoridade Nacional de Proteção de dados. **ANPD torna-se membro da Rede Ibero-Americana de proteção de dados**. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-membro-da-rede-ibero-america-de-protecao-de-dados>. Acesso em: 09 mar. 2023.

BRASIL. Empresa Brasileira de Serviços Hospitalares. **Robôs virtuais de hospitais da Rede Ebserrh/MEC fizeram quase nove mil atendimentos que auxiliam no combate à Covid-19**. 2021. Disponível em: <https://www.gov.br/ebserrh/pt-br/comunicacao/noticias/robos-virtuais-de-hospitais-da-rede-ebserrh-mec-fizeram-quase-nove-mil-atendimentos-que-auxiliam-no-combate-a-covid-19>. Acesso em: 27 dez. 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Estratégia Brasileira de Inteligência Artificial**. 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf. Acesso em: 12 jan. 2023.

BRASIL. Autoridade Nacional de Proteção de dados. **Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico_defeso_eleitoral.pdf. Acesso em: 12 dez. 2022.

BRASIL. Diário Oficial. **Portaria ANPD nº 35, de 4 de novembro de 2022**. 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885>. Acesso em: 12 dez. 2022.

BRASIL. Senado Federal. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022.

BRASIL. Senado Federal. **CJSUBIA**. [S.l.]. Disponível em: <https://legis.senado.leg.br/comissoes/comissao?codcol=2504>. Acesso em: 17 jan. 2023.

BROWNEE, Jason. **What is semi-supervised learning**. 2021. Disponível em: <https://machinelearningmastery.com/what-is-semi-supervised-learning/>. Acesso em: 06 fev. 2023.

BURRELL, Jenna. How the machine ‘thinks’: Understanding opacity in machine learning algorithms. **Big data and Society**, jan.-jun., 2016.

CASEY, Bryan; FARHANGI, Ashkon; VOGLP, Roland. Rethinking explainable machines: the GDPR’s right to explanation debate and the rise of algorithm audits in enterprise. **Berkeley Technology Law Journal**, v. 34, 2019.

CHOI, Jin-A; LIM, Kiho. Identifying machine learning techniques for classification of target advertising. **ICT Express**, v. 6, n. 3, 2020, p. 175-180.

COLUMBIA UNIVERSITY. **The Case of Lebach**. s.d. Disponível em: <https://globalfreedomofexpression.columbia.edu/cases/the-case-of-lebach/>. Acesso em: 26 jan. 2023.

COLÔMBIA. Consejería Presidencial para Asuntos Económicos y Transformación Digital. **Marco Ético para la Inteligencia Artificial en Colombia**. 2020. Disponível em: <https://www.usergioarboleda.edu.co/wp-content/uploads/2021/11/Marco-etico-para-la-inteligencia-artificial-en-Colombia-Maestria-en-Inteligencia-artificial.pdf>. Acesso em: 11 jan. 2023.

CORMEN, Thomas H. *et al.* **Introduction to algorithms**. 3. ed. Cambridge: The MIT Press, 2009.

CRAWFORD, Kate. **Atlas of AI: Poder, Politics and the Planetary Costs of Artificial Intelligence**. New Haven: Yale University Press, 2021.

CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. **Boston College Law Review**, vol. 55, 2014.

CUEVA, Ricardo Villas Bôas. Banco de dados e cadastros de consumidores no Código de Defesa do Consumidor: da privacidade à proteção de dados pessoais. **Revista do Advogado**, ano XL, n. 147, setembro de 2020.

DASTIN, Jeffrey. **Amazon scraps secret AI recruiting tool that showed bias against women**. 2018. Disponível em: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>. Acesso em: 31 jan. 2023.

DINAMARCA. Datatilsynet. **2019-421-0028**. Publicado em: 26.02.2020. Disponível em: https://gdprhub.eu/index.php?title=Datatilsynet_-_2019-421-0028. Acesso em: 28 dez. 2022.

DINAMARCA. Datatilsynet. **Artificial intelligence and privacy**. 2018. Disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Acesso em: 06 fev. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo *et al.* Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018. Disponível em: <https://ojs.unifor.br/rpen/article/view/8257/pdf>. Acesso em: 20 dez. 2022.

DONEDA, Danilo; VIOLA, Mario. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. **Revista Brasileira de Risco e Seguro**, Rio de Janeiro, v. 5, n. 10, p. 85-102, out. 2009/mar. 2010. Disponível em: <https://www.rbrs.com.br/arquivos/RBRS10-4%20Danilo%20Doneda.pdf>. Acesso em: 11 nov. 2022.

DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. CUEVA, Ricardo Villas Bôas Cueva; DONEDA, Danilo; MENDES, Laura Schertel

(coord.). **Lei geral de proteção de dados** (Lei nº 13.709/2018): a caminho da efetividade, contribuições para a implementação da LGPD. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

DOSHI-VELEZ, Finale *et al.* Accountability of AI Under the Law: The Role of Explanation. **arXiv:1711.01134**. 2019, p. 21 Disponível em: <https://doi.org/10.48550/arXiv.1711.01134>. Acesso em: 15 mar. 2023.

DLA PIPER. **Data Protection Laws of the World**. 2022. Disponível em: <https://www.dlapiperdataprotection.com/>. Acesso: 15 jul. 2022.

EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a “right to explanation” is probably not the remedy you are looking for. **Duke Law and Technology Review**, v. 16, n. 1, 2017.

EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”? **IEEE Security & Privacy**, v. 16, n. 3, 2018.

ESTADOS UNIDOS DA AMÉRICA. Department of Health, Education and Welfare. **Records, Computers and the Rights of Citizens**, 1973. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 10 nov. 2022.

ESTADOS UNIDOS DA AMÉRICA. **Preparing for the future of artificial intelligence**. 2016. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NS-TC/preparing_for_the_future_of_ai.pdf. Acesso em: 22 nov. 2022.

FLORENCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. **Suprema: revista de estudos constitucionais**, v. 1, n. 1, p. 154-180, jan./jun. 2021. Disponível em: <https://suprema.stf.jus.br/index.php/suprema/article/view/20/18>. Acesso em: 29 dez. 2022.

FOWLER, Geoffrey. I tried to read all my app privacy policies. It was 1 million words. 2022. Disponível em: <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>. Acesso em: 13 jun. 2023.

FRAZÃO, Ana. **Decisões algorítmicas e direito à explicação**. Em que medida é possível encontrar explicações em decisões algorítmicas? 2021. Disponível em: http://www.professoraanafraza.com.br/files/publicacoes/2021-11-24-Decisoes_algoritmicas_e_direito_a_explicacao_Em_que_medida_e_possivel_encontrar_explicacoes_em_decisoes_algoritmicas.pdf. Acesso em: 11 nov 2022.

FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais Fundamentos da LGPD**. 1ª. ed. Rio de Janeiro: Forense, 2022.

FINLÂNDIA. Tietosuojavaltuutetun toimisto. **3895/83/22**. Julgado em: 23.06.2022. Disponível em: https://gdprhub.eu/index.php?title=Tietosuojavaltuutetun_toimisto_%28Finland%29_-_3895%2F83%2F22. Acesso em: 27 dez. 2022.

FUENTES, Patricio Velasco; VENTURINI, Jamila. **Decisões automatizadas na gestão pública na América Latina**. 2021, p. 27. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/08_Informe-Comparado-PT_180222.pdf. Acesso em: 16 dez. 2022.

GAMBOGI, Ana Paula. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (org.). **Coleção doutrinas essenciais**: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 915-954.

GARTNET. **Gartner Glossary**. [s.d]. Disponível em: <https://www.gartner.com/en/information-technology/glossary/big-data>. Acesso em: 19 dez. 2022.

GILLESPIE, Tarleton. The Relevance of Algorithms. In: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo; FOOT, Kirsten. **Media Technologies**. Cambridge: MIT Press, 2013.

GILIS, Talia B. The Input Fallacy. **Minnesota Law Review**. 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571266. Acesso em: 17 jan. 2023.

GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”. **AI MAGAZINE**, 2017.

GRAVINA, Maurício Salomoni. **Princípios Jurídicos do Contrato de Seguro**. Rio de Janeiro, Funenseg, 2015.

GREGGARD, Samuel. **What is Artificial Intelligence & How Does It Work?** 2019. Disponível em: <https://www.datamation.com/artificial-intelligence/what-is-artificial-intelligence>. Acesso em: 27 jan. 2023.

GREENLEAF, Graham; COTTIER, Bertil. 2020 Ends a Decade of 62 New Data Privacy Laws. **163 Privacy Laws & Business International Report 24-26**. 2020. Disponível em: <https://deliverypdf.ssrn.com/delivery.php?ID=527000067124025069095112078067099108039003024042071075093075112088116126097095002067114102007027106035006118101120066003025084005082039040022083030076122096006008064047024093092031069065113120083080117087014081023065111025111126073009092030007102&EXT=pdf&INDEX=TRUE>. Acesso em: 14 nov. 2022.

GUTIÉRREZ, Juan David; MUÑOZ-CADENA, Sarah. Sistemas de decisión automatizada implementados por el Estado Colombiano. **XI Congreso Internacional en Gobierno, Administración y Políticas Públicas GIGAPP**, Madrid, España, del 21 al 23 de septiembre de 2022.

HAO, Karen. This is how AI bias really happens – and why it’s so hard to fix. **MIT Technology Review**, 2014. Disponível em: <https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/>. Acesso em: 30 dez. 2022.

HANKIEWICZ, Kamila. **What Is The Real Difference Between Automation And AI?** 2018. Disponível em: <https://becominghuman.ai/what-is-the-real-difference-between-automation-and-ai-366513e0c910>. Acesso em: 2022.

HARARI, Yuval. **Yuval Noah Harari on big data, Google and the end of free will**. 2016. Disponível em: <https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c>. Acesso em: 29 dez. 2022.

PAÍSES BAIXOS. RB Den Haag. **CC/09/585239/ KG ZA 19/1221**. Julgado em: 11.02.2020. Disponível em: https://gdprhub.eu/index.php?title=Rb._Den_Haag_-_C/09/585239/_KG_ZA_19/1221. Acesso em: 16.02.2023.

PAÍSES BAIXOS. Rechtbank Amsterdam. **C/13/687315 / HA RK 20-207**. Julgado em 11.03.2021. Disponível em: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/687315/_HA_RK_20-207. Acesso em: 26 dez. 2022.

PAÍSES BAIXOS. Rechtbank Amsterdam. **C/13/692003/HA RK 20-302**. Julgado em: 11.03.2021. Disponível em: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/692003/HA_RK_20-302. Acesso em: 26 dez. 2022.

HUBMANN Heinrich. **Das Persönlichkeitsrecht**. 2ª. ed. Colônia: 1967.

ITÁLIA. Garante per la Protezione dei Dati Personali. **9675440**. Julgado em: 10.06.2021. Disponível em:

[https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-9675440](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-9675440). Acesso em: 27 dez. 2022.

ITÁLIA. Garante per la Protezione dei Dati Personali. **9685994**. Julgado em: 22.07.2021. Disponível em: [https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-9685994](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-9685994). Acesso em: 27 dez. 2022.

KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019.

KHANDELWAL, Renu. **Supervised, Unsupervised, and Reinforcement Learning**. 2019. Disponível em: <https://arshren.medium.com/supervised-unsupervised-and-reinforcement-learning-245b59709f68>. Acesso em: 21 dez. 2022.

KOCHENDERFER, Mykel; WHEELER, Tim; WRAY, Kyle. **Algorithm for Decision Making**. Massachusetts: The MIT Press, 2022. Disponível em: <https://algorithmsbook.com/files/dm.pdf>. Acesso em: 21 dez. 2022.

KOZYRKOV, Cassie. **Explainable AI won't deliver. Here's why**. 2018. Disponível em: <https://kozyrkov.medium.com/explainable-ai-wont-deliver-here-s-why-6738f54216be>. Acesso em: 16 jan. 2023.

KOZYRKOV, Cassie. **Are you using the term AI incorrectly?** 2018. Disponível em: <https://hackernoon.com/are-you-using-the-term-ai-incorrectly-911ac23ab4f5>. Acesso em: 06 fev. 2023.

KUMAS, Yogesh *et al.* Artificial intelligence in disease diagnosis: a systematic literature review, synthesizing framework and future research agenda. **Journal of Ambient Intelligence and Humanized Computing**, Springer, 2022.

LAZARO, Christophe; LE MÉTAYER, Daniel. **Control over personal data: true remedy or fairy tale?** SCRIPTed, vol. 12, issue 1, 2015. Disponível em: <https://script-ed.org/article/control-over-personal-data-true-remedy-or-fairy-tale/>. Acesso em 11 nov. 2022.

LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, v. 26, p. 227-246, out./dez. 2020.

LUDER, Amanda. **Robô que analisa processos do INSS causa aumento de recursos por indeferimento**. 2022. Disponível em: <https://g1.globo.com/economia/noticia/2022/10/07/robo-que-analisa-processos-do-inss-causa-aumento-de-recursos-por-indeferimento.ghtml>. Acesso em: 27 dez. 2022.

MACEDO, André Batisti de; SCHMIDT, Roberto Eurico. **O Regime de Responsabilidade Civil aplicado na Lei Geral de Proteção de Dados**. [S.l.]. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/25299/1/ARTIGO.pdf>. Acesso em: 1 mar. 2023.

MALGIERI, Gianclaudio. Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations. **Computer Law and Security Review**, n. 35, 2019.

MATTIUZZO, Marcela. **O carro na frente dos bois: a precipitada regulação da IA no Brasil**. 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/fronteiras-concorrencia-regulacao/precipitada-regulacao-da-inteligencia-artificial-no-brasil-26082021>. Acesso em: 17 jan. 2023.

MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005. Disponível em: <https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs>

[-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf](#).

Acesso em: 11 nov 2022.

MARTINS, Alessandra Ferreira. **Exame de proporcionalidade nos casos de colisão de direitos fundamentais**. Monografia (Graduação) - Faculdade de Direito da Universidade Federal do Paraná, 2003. Disponível em:

<https://acervodigital.ufpr.br/bitstream/handle/1884/44913/M221.pdf?sequence=1&isAllowed=y>. Acesso: 10 nov. 2022.

MARTINS, Pedro Bastos Lobo; HOSNI, David Salim Santos. Tomada de Decisão Automatizada e a Regulamentação da Proteção de Dados: Alternativas Coletivas Oferecidas pela Lei Geral de Proteção de Dados. **Revista Internet e Sociedade**, v. 1, n. 2, dez. 2020.

Disponível em: <https://revista.internetlab.org.br/736-2/>. Acesso em: 23 mar. 2023.

MASOLO, Cláudio. **Supervised, unsupervised and deep learning**. 2017. Disponível em: <https://towardsdatascience.com/supervised-unsupervised-and-deep-learning-aa61a0e5471c>.

Acesso em: 21 dez. 2022.

MAYER-SCHONEBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip; ROTENBERG, Marc. (ed.). **Technology and Privacy**. The New Landscape. Cambridge: MIT Press, 1997.

MCFARLAND, Matt. **Terrorist or pedophile? This start-up says it can out secrets by analyzing faces**. 2016. Disponível em:

<https://www.washingtonpost.com/news/innovations/wp/2016/05/24/terrorist-or-pedophile-this-start-up-says-it-can-out-secrets-by-analyzing-faces/>. Acesso em: 14 dez. 2022.

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

MENDES, Laura Schertel; BIONI, Bruno Ricardo. 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**. vol. 124. ano 28, p. 157-180. São Paulo: ed. RT, jul.-ago. 2019.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado) - Faculdade de Direito da Universidade de Brasília, 2008. Disponível em:

<https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso: 10 nov. 2022.

MENDES, Laura Schertel. 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/view/10828/pdf>. Acesso em: 16 nov. 2022.

MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **RDU**, Porto Alegre, Volume 16, n. 90, 2019, 39-64, nov-dez 2019.

MENDES, Gilmar Ferreira; GONET BRANCO, Paulo Gustavo; **Curso de Direito Constitucional**. 14ª. ed. São Paulo: Saraiva Educação, 2019.

MENDOZA, Isak; BYGRAVE, Lee. The Right not to be Subject to Automated Decisions based on Profiling. In: SYNODINOU, Tatiani *et al.* (eds.). **EU Internet Law: Regulation and Enforcement**. [s.l]: Springer, 2017.

MERCOSUL. **Protección de datos personales y su libre circulación**. 2010. Disponível em: https://documentos.mercosur.int/simfiles/proynormativas/24606_SGT13_2010_ACTA01_AN

[E04_PDecS-N_ES_Protecci%C3%B3n%20Datos%20Personales.pdf](#). Acesso em: 14 nov. 2022.

MITTELSTADT, Brent; RUSSELL, Chris; WACHTER, Sandra. Explaining Explanations in AI. **FAT* '19: Conference on Fairness, Accountability, and Transparency**, January, 2019, Atlanta, Georgia, USA.

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

MOLNAR, Christoph. **Interpretable Machine Learning**: a guide for making black box models explainable. 2ª. ed. 2022. Disponível em:

<https://christophm.github.io/interpretable-ml-book/>. Acesso em: 05 jan. 2023.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência artificial e a lei de proteção de dados pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: FRAZÃO, Ana. MULHOLLAND, Caitlin (Coord.).

Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019.

NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus. Journal of the American Academy of Arts and Sciences**, v. 140, n. 4, 2011.

NOUGRÈRES, Ana Brian. El sistema legal uruguayo de protección de datos personales. **Revista de Derecho, Comunicaciones y Nuevas Tecnologías**, 2007.

OCDE. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. 2013. Disponível em:

<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#:~:text=Personal%20data%20should%20be%20protected,modification%20or%20disclosure%20of%20data..> Acesso em: 12 dez. 2022.

OCDE. **OECD AI Principles**. 2019. Disponível em: <https://oecd.ai/en/ai-principles>. Acesso em: 11 nov. 2022.

OCDE. **Artificial Intelligence**. Paris: OECD Publishing, 2019. The technical landscape. Disponível em:

<https://www.oecd-ilibrary.org/sites/eedfee77-en/1/2/1/index.html?itemId=/content/publication/eedfee77-en&csp=5c39a73676a331d76fa56f36ff0d4aca&itemIGO=oecd&itemContentType=book> Acesso em: 21 dez. 2022.

OCDE. **Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe**. Paris: OECD Publishing, 2022.

O'NEIL, Cathy. **Weapons of math destruction - how big data increases and threatens democracy**. Nova York: Crown, 2016.

PASQUALE, Frank. **The Black Box Society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PASQUALE, Frank. Restoring transparency to automated authority. **Journal on Telecommunication and High Technology Law**, v. 9, n. 235, 2011.

PEHLÍVAN, Ceyhun. Data Protection in Latin America: an overview. **Global Privacy Law Review**, v. 2, n. 2. The Netherlands: Kluwer Law International BV, 2021.

PEREIRA DA SILVA, Sivaldo; CESAR, Daniel Jorge Teixeira. Inteligência Artificial, moderação de conteúdos no YouTube e a proteção de direitos: características, problemas e impactos políticos. **Liinc em Revista**, Rio de Janeiro, v. 18, n. 2, e6080, nov. 2022.

PRIVACIDADE HACKEADA. **Direção de Karim Amer e Jehane Noujaim**. Estados Unidos: Netflix, 2019. (110 min)

PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária accountability. **Revista de Informação Legislativa**, v. 57, n. 225, p. 43-60, jan./mar. 2020, p. 58. Disponível em:

https://www12.senado.leg.br/ril/edicoes/57/225/ril_v57_n225_p43.pdf. Acesso em: 29 dez. 2022.

PONT, Vivian Newman; ARANGO, María Paula Ángel. **Rendición de cuentas de Google y otros negocios en Colombia**: la protección de datos personales en la era digital. 2019.

Disponível em:

<https://www.dejusticia.org/wp-content/uploads/2019/01/Rendicio%CC%81n-de-cuentas-de-Google-y-otros-negocios-en-Colombia.pdf>. Acesso em: 11 jan. 2023.

QUELLE, Claudia, Not just user control in the General Data Protection Regulation. On the problems with choice and paternalism, and on the point of data protection, Karlstad: Springer, 2017. In: LEHMANN, A.; *et al.* (orgs.). **Privacy and Identity Management - Facing up to Next Steps**. Karlstad: Springer, 2017.

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. **Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial**. 2019, p. 21. Disponível em:

[https://www.sic.gov.co/sites/default/files/files/pdf/2%20RIPD%20\(2019\)%20GENERAL%20RECOMMENDATIONS%20FOR%20THE%20PROCESSING%20OF%20PERSONAL%20DATA%20IN%20ARTIFICIAL%20INTELLIGENCE\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/2%20RIPD%20(2019)%20GENERAL%20RECOMMENDATIONS%20FOR%20THE%20PROCESSING%20OF%20PERSONAL%20DATA%20IN%20ARTIFICIAL%20INTELLIGENCE(1).pdf). Acesso em: 11.02.2023.

REDAÇÃO FORBES. Com coronavírus, redes sociais alertam para possíveis erros de moderação de conteúdo. **Forbes**. 2020. Disponível em:

<https://forbes.com.br/negocios/2020/03/com-coronavirus-redes-sociais-alertam-para-possiveis-erros-de-moderacao-de-conteudo/>. Acesso em: 15 dez. 2022.

REMOLINA-ANGARITA, Nelson. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz de estándar europeo?. **Revista Colombiana de Derecho Internacional**, n. 16, p. 489-524, 2010.

REINO UNIDO. Government Office for Science. **Artificial intelligence: opportunities and implications for the future of decision making**. 2016. Disponível em:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf. Acesso em: 19 dez. 2022.

REINO UNIDO. Information Commissioner's Office. **Big data, artificial intelligence, machine learning and data protection**. 2017. Disponível em:

<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Acesso em: 19 dez. 2022.

REINO UNIDO. Information Commissioner's Office. **Rights related to automated decision making including profiling**. [s.d]. Disponível em:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>. Acesso em: 11 nov. 2022.

REINO UNIDO. Information Commissioner's Office. **Guide to the General Data Protection Regulation**. 2022. Disponível em:

<https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>. Acesso em: 07 dez. 2022.

REINO UNIDO. Information Commissioner's Office. **Explaining decisions made with IA**. 2022. Disponível em:

<https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf>. Acesso em: 14 mar. 2023.

REIS, Carolina *et al.* **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil**. Brasília: Laboratório de Políticas Públicas e Internet, 2021, p. 56 - 59.

REIGADA, Antonio Troncoso. El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección

de datos a nivel internacional. **Revista Latinoamericana de Protección de Datos Personales**, n. 5, 2018.

RIBEIRO, Marco Tulio; SINGH, Sameer; GUESTRIN, Carlos. "Why Should I Trust You?": Explaining the Predictions of Any Classifier. **Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, ACM Press, 2016, p. 1135–1144.

RITSCHER, Chelsea. 'Female only' app criticised as 'transphobic' and 'racist' after AI software denies some women. 2022. Disponível em: <https://www.independent.co.uk/life-style/female-only-app-giggle-transphobic-b2002235.html>. Acesso em: 14 dez. 2022.

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

ROIG, Antoni, Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). **European Journal of Law and Technology**, v. 8, n. 3, 2017.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: a modern approach**. 4. ed. Reino Unido: Pearson, 2022.

SARDINHA, Adrine Nascimento Celestino. **Direito à informação e à revisão de decisões informatizadas: uma análise da LGPD**. Poro Alegre, v. 6, n. 2, p. 257-286, mai. 2022.

SARLET, Ingo W.; DONEDA, Danilo; MENDES, Laura S. **Estudos sobre proteção de dados pessoais. (Coleção Direito, tecnologia, inovação e proteção de dados num mundo em transformação)**. São Paulo: Editora Saraiva, 2022.

SCHWARTZ, Paul; SOLOVE, Daniel; The PII Problem: Privacy and a new concept of personally identifiable information. **New York University Law Review**, v. 86, 2011, p. 1814.

SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017.

SILVA, Tarcízio. Linha do Tempo do Racismo Algorítmico. **Blog do Tarcízio Silva**, 2022. Disponível em: <https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo>. Acesso em: 12 dez. 2022.

SILVA, Priscilla; MEDEIROS, Juliana. **A polêmica da revisão (humana) sobre decisões automatizadas**. 2019. Disponível em: <https://feed.itsrio.org/a-pol%C3%AAmica-da-revis%C3%A3o-humana-sobre-decis%C3%B5es-automatizadas-a81592886345>. Acesso em: 21 dez. 2022.

SIMONITE, Tom. **Skewed Grading Algorithms Fuel Backlash Beyond the Classroom**. 2020. Disponível em: <https://www.wired.com/story/skewed-grading-algorithms-fuel-backlash-beyond-classroom/>. Acesso em: 28 dez. 2022.

SOUZA, Carlos Affonso; PERONE, Christian; MAGRANI, Eduardo. O direito à explicação: entre a experiência europeia e a sua posituação na LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

SOUZA, Maique Barbosa de. **Governança em bancos de dados de análise de crédito para instituições financeiras a partir do uso da inteligência artificial e das decisões automatizadas**: como a adequação interna pode contribuir para a correta definição do risco representado no score de crédito. Dissertação (mestrado) Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, Porto Alegre, 2022.

SOLOVE, Daniel. Privacy Self-Management and the consent Dilemma. **Harvard Law Review**, v. 126, 2013.

SOLOVE, Daniel. *The Limitations of Privacy Rights*. **GW Law Faculty Publications and Other Works**, 2022.

STEINMULLER *et al.* **Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern**. BTdrucks VI/326, anexo 1, 1972. Disponível em: <https://dserver.bundestag.de/btd/06/038/0603826.pdf>. Acesso em: 11 nov. 2022.

STOHL, Cynthia; STOHL, Michael; LEONARDI, Paul M. Digital Age Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age. **International Journal of Communication**, [S.l.], v. 10, p. 15, jan. 2016. ISSN 1932-8036. Date accessed: 16 jan. 2023.

TAVARES, Leticia Antunes; ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. In: ONODERA, Marcus Vinicius (coord.); DE FILIPPO, Thiago Baldani (coord.). **Brasil e EUA: Temas de direito comparado**. São Paulo: Escola Paulista da Magistratura, 2017.

TAVARES, Clarice *et al.* **O Auxílio Emergencial no Brasil: Desafios na implementação de uma política de proteção social datificada**. 2022. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/01_Informe-Brasil_Inteligencia-Artificial-e-Inclusao_PT_22042022.pdf. Acesso em: 15 dez. 2022.

TRANSPARÊNCIA BRASIL. **Uso de Inteligência Artificial pelo Poder Público. Recomendações de Governança**. 2020. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_I_A_PoderPublico.pdf. Acesso em: 26 dez. 2022.

TUROW, Joseph. **The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth**. Yale University Press, 2011.

UNESCO. **Ad Hoc Expert Group (AHEG) for the preparation of a draft text of a recommendation on the ethics of artificial intelligence**. 2020. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000373434>. Acesso em: 11 nov. 2022.

UNIÃO EUROPEIA. Parlamento Europeu. **Directiva 95/46/CE** do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 10 jan. 2023.

UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 3/2010 on the principle of accountability**. 2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Acesso em: 12 dez. 2022.

UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Opinion 03/2013 on purpose limitation**. 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 13 dez. 2022.

UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Transparency under Regulation 2016/679**. 2016. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>. Acesso em: 13 dez. 2022.

UNIÃO EUROPEIA. Article 29 Data Protection Working Party. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. 2017. Disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963. Acesso em: 14 dez. 2022.

UNIÃO EUROPEIA. European Union Agency for Fundamental Rights. **Handbook on European data protection law**. Luxembourg: Publications Office of the European Union, 2018.

UNIÃO EUROPEIA. Conselho da Europa. **128th Session of the Committee of Ministers**. 2018. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf. Acesso em: 09 jan. 2023.

UNIÃO EUROPEIA. Conselho da Europa. **Artificial Intelligence and data protection**. 2019. Disponível em: <https://rm.coe.int/2018-lignes-directrices-sur-l-intelligenceartificielle-et-la-protecti/168098e1b7>. Acesso em: 29 dez. 2022.

UNIÃO EUROPEIA. European Insurance and Occupational Pensions Authority. **Big data analytics in motor and health insurance: a thematic review**. Luxembourg: Publications Office of the European Union, 2019.

UNIÃO EUROPEIA. Comissão Europeia. **A definition of Artificial Intelligence: main capabilities and scientific disciplines**. High-Level Expert Group on Artificial Intelligence. 2019. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Acesso em: 20 dez. 2022.

UNIÃO EUROPEIA. Comissão Nacional de Proteção de Dados. **Deliberação/2021/622**. Julgado em: 11.05.2021. Disponível em: <https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887>. Acesso em: 28 dez. 2022.

UNIÃO EUROPEIA. Comissão Europeia. **Data protection in the EU**. 2021. Disponível em: [https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#:~:text=The%20European%20Data%20Protection%20Board,Data%20Protection%20Regulation%20\(GDPR\)](https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#:~:text=The%20European%20Data%20Protection%20Board,Data%20Protection%20Regulation%20(GDPR)). Acesso em: 16 dez. 2022.

UNIÃO EUROPEIA. European Union Agency for Fundamental Rights. **Bias in Algorithms – Artificial Intelligence and Discrimination**. Luxembourg: Publications Office of the European Union, 2022.

URUGUAI. Unidad Reguladora y de Control de Datos Personales. **Guía General de Protección de Datos Personales en Uruguay**. 2022. Disponível em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-general-proteccion-datos-personales-uruguay>. Acesso em: 10 jan. 2023.

URUGUAI. Ministério de Salud Publica. **Información sobre la Aplicación Coronavirus UY**. 2020. Disponível em: <https://www.gub.uy/ministerio-salud-publica/politicas-y-gestion/informacion-sobre-aplicacion-coronavirus>. Acesso em: 10 jan. 2023.

URUGUAI. Ministério de Salud Publica. **Guía para usuarios de la aplicación Coronavirus UY**. 2020. Disponível em: https://www.gub.uy/ministerio-salud-publica/sites/ministerio-salud-publica/files/2020-06/diseño%CC%83o%20gacetilla%20coronavirus%20%20copia_0.pdf. Acesso em: 10 jan. 2023.

VÁSQUEZ, Carolina Sánchez. **El derecho al control humano en la inteligencia artificial**. Una propuesta de regulación del control humano como un nuevo derecho en el ordenamiento jurídico colombiano. Universidad EAFIT, 2021.

VERONESE, Alexandre. Capítulo 14. Os direitos de explicação e de oposição diante das decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual explanations without opening the black box: automated decisions and the GDPR. **Harvard Journal of Law & Technology**, v. 31, n. 2, Spring, 2018.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age on big data and AI. **Columbia Business Law Review**, 2019.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, vol. , n. 5, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 10 nov. 2022.

WESTIN, Alan. **Privacy and freedom**. New York: Ig Publishing, 1967, p. 24. Disponível em: <https://dokumen.pub/privacy-and-freedom-1632460734-9781632460738.html>. Acesso em: 11 nov. 2022.

ZABALA LEAL, Tatiana Dulima. La ética en inteligencia artificial desde la perspectiva del Derecho. **Via Inveniendi Et Iudicandi**, v. 16, n. 2, 2021.

ZANATTA, Rafael. **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. 2019. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais?channel=doi&linkId=5c7078f8a6fdcc4715941ed7&showFulltext=true. Acesso em: 23 mar. 2023.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. Estados Unidos: Perseus Books, LLC, 2021.